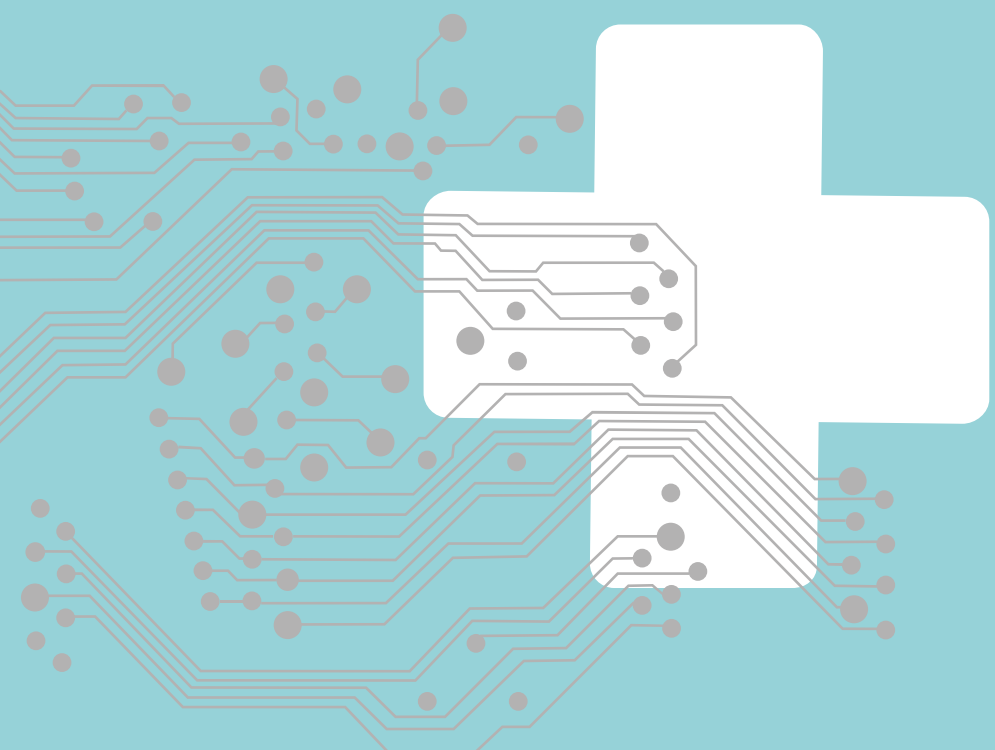
EHEALTHCOMPASS

IT-SICHERHEIT

Cyberattacke im Krankenhaus · IT-Sicherheit und der Faktor Mensch · Patientendaten auf dem Schwarzmarkt · Erfahrungen aus der Krankenhaus-IT-Leitung · Datenschutz und Health Apps · Sichere IT-Systeme · Schutz nach dem IT-Sicherheitsgesetz

EHEALTHCOM



conhIT

25.–27. April 2017

Connecting Healthcare IT

www.conhit.de

Industrie-Messe
Kongress
Akademie
Networking

Call for Papers 2017

Gestalten Sie den conhIT-Kongress 2017 mit – präsentieren Sie Ihr Thema!

In der Zeit vom **17. Oktober 2016 bis zum 18. November 2016** können Sie Ihre Themen unter www.conhit.de einreichen.

In Kooperation mit

Unter Mitwirkung von

Veranstalter

Organisation

Laut des IBM Cyber Security Intelligence Index 2016 steht die Gesundheitsbranche auf Platz eins der am meisten attackierten Industrien. Der hohe Digitalisierungsgrad moderner Krankenhäuser und die zunehmende Vernetzung im Gesundheitswesen machen zwar effektiv, aber auch verwundbar! Das haben nicht zuletzt die Cyberangriffe an deutschen Krankenhäusern Anfang des Jahres gezeigt. Doch welche Krankenhausbereiche sind besonders gefährdet und wie lassen sich diese erkennen? Welche typischen Gefährdungen sollte jeder kennen? Welche Rolle spielt der Faktor Mensch? Es gilt, Lösungsansätze zu finden, die einerseits die Datensicherheit garantieren und andererseits eine Vernetzung des Gesundheitswesens zulassen.

Die Beiträge des ersten E-HEALTH-COMPASS zur IT-Sicherheit spiegeln die verschiedenen Aspekte und Einschätzungen zu diesem Themenkomplex wider: Von dem Bericht eines von einer Cyberattacke betroffenen Krankenhauses über die Vorstellung eines Forschungsprojekts, das den Faktor Mensch in den Mittelpunkt stellt, sowie die Perspektive eines Krankenhaus-IT-Leiters bis hin zu aktuellen Zahlen und Einschätzungen zu Patientendaten auf dem Schwarzmarkt sowie zum Thema Datenschutz bei Health Apps. Die Beiträge und Analysen zeigen: Die Bedrohung ist ernst zu nehmen, aber es sollte nicht dramatisiert werden. Denn Deutschland ist im Vergleich zu anderen Ländern (insbesondere den USA) noch nicht so stark von Angriffen Cyberkrimineller betroffen. Das schafft zumindest einen gewissen Zeitpuffer, um aus den bisherigen Erfahrungen und Versäumnissen zu lernen und Vorkehrungen zur Vorbeugung zu treffen (wie es u.a. die Bundesregierung mit dem IT-Sicherheitsgesetz und der gerade in Arbeit befindlichen KRITIS-Verordnung für Betreiber Kritischer Infrastrukturen im Gesundheitswesen tut). Denn: Gesundheitsdaten sind ein hoch sensibles und schützenswertes Gut. Und das sollte weiterhin oberste Priorität bei allen Beteiligten sein.

Ich wünsche allen Leserinnen und Lesern eine anregende und erkenntnisreiche Lektüre.

ANNE WOLF
Projektleitung,
Redaktion E-HEALTH-COM

THEMEN

04 CYBERATTACKE
IT-Ausfall im Krankenhaus

08 KRANKENHAUS-IT
IT-Sicherheit und der Faktor Mensch

18 IT-SICHERHEIT
IT-Sicherheit im Krankenhaus

22 CYBERKRIMINALITÄT
Patientendaten auf dem Schwarzmarkt

25 DATENSCHUTZ & HEALTH APPS
Im Fokus der Hacker: Gesundheitsdaten

29 IMPRIVATA
5 Schritte für sichere IT-Systeme

30 VIDEC.
Effizienter Schutz nach dem IT-Sicherheitsgesetz

IMPRESSUM

Herausgeber: Hans-Peter Bröckerhoff | **Redaktion:** Anne Wolf (Projektleitung, v.i.S.d.P.), Silke Weidner (Korrektorat) | **Grafik:** Berta Mattern | **Anzeigen:** Beate Gehm, Tel.: +49-(0)69-840 006-3030, Mail: b.gehm@health-care-com.de | **Anschrift Redaktion und Verlag:** HEALTH-CARE-COM GmbH, Redaktion E-HEALTH-COM, Goethering 58, 63067 Offenbach | Tel.: +49-(0)69-840 006-3020, www.e-health-com.eu | Mail: redaktion@e-health-com.eu | **Druck:** Kössinger AG, Schierling | **Auflage:** 14 000 Exemplare; die Hälfte davon beigelegt in dem Magazin E-HEALTH-COM

IT-Ausfall im KRANKENHAUS

Am Neusser Lukaskrankenhaus ereignete sich Anfang des Jahres ein Angriff durch Schadsoftware. Welche Auswirkungen hatte dies auf die Alltagsroutine in der Radiologie, welche Maßnahmen wurden akut getroffen und wie ging es danach weiter? Ein Erfahrungsbericht.

TEXT: MATHIAS COHNEN

© LUKASKRANKENHAUS

Digitale Datenverarbeitung ist seit vielen Jahren ein wichtiger Motor der Entwicklung auch im Gesundheitswesen. Die Verfügbarkeit von personenbezogenen Daten muss plattformübergreifend und damit in einem hohen Grad an Vernetzung verfügbar sein. Im Gegenzug wird seit vielen Jahren jedoch sowohl im privaten wie auch im öffentlich-rechtlichen und wirtschaftlichen Bereich vor Cyberkriminalität gewarnt, wobei ein hoher Komplexitäts- und Vernetzungsgrad Angriffe nicht nur einfacher, sondern auch wirkungsvoller werden lässt.

Cyberattacke und ihre Folgen für die Radiologie

Der folgende Beitrag stellt die Folgen einer Attacke durch Schadsoftware (Ransomware) auf die Radiologie eines mittelgroßen Schwerpunktkrankenhauses (>500 Betten, CPU, Intensivstation mit 20 Beatmungsbetten, zentrale Notaufnahme mit >50 000 Patientenkontakten pro Jahr, Onkologie) dar. Am frühen Morgen eines Werktages fielen vereinzelt verlangsamte IT-Prozesse auf, insbesondere ein Ausfall des CD-Brenn-Servers. Bei der Analyse durch die IT-Abteilung wurden auch in anderen Systemen Prozessunregelmäßigkeiten wahrgenommen, die schnell auf einen Angriff durch Schadsoftware zurückgeführt werden konnten: Zu beobachten war eine Verschlüsselung von Dateien aus dem Office-Bereich, aber auch von PDF-Dokumenten sowie von Bilddateien sowohl auf peripheren PCs als auch zentralen Servern. Die besondere Aggressivität der Schadsoftware ergab sich aus der raschen Verteilung über das gesamte Netzwerk zwischen einzelnen Clients, aber auch den teilweise virtualisierten Servern. Die Ransomware, die in kurzen Zeitabständen ihre Signatur änderte, konnte durch die bis dahin eingesetzten professionellen Virenscanner nicht identifiziert werden.

Um einen Datenverlust zu vermeiden und die weitere Ausbreitung zu beenden, wurden daher alle Server notfallmäßig, aber geordnet heruntergefahren, sodass innerhalb weniger als einer halben Stunde sämtliche IT-Systeme krankenhausweit nicht mehr zur Verfügung standen. Zeitgleich wurden sämtliche Netzwerke einschließlich der Knotenpunkte deaktiviert. Alle peripheren Computer im Krankenhaus mussten abgeschaltet werden und durften bis auf Weiteres nicht mehr in Betrieb genommen werden.

Entsprechend dem Notfallplan des Krankenhauses wurde diese Situation als vergleichbar einem ausgedehnten Stromausfall angesehen und analog verfahren. Der erweiterte Krisenstab stufte die Tragweite der Krisensituation als erheblich und potenziell patientengefährdend ein. In einem ersten Schritt wurde daher die Neuaufnahme von kritisch kranken Patienten unterbrochen. Die manuelle Versorgung der intensivmedizinisch behandelten Patienten war zu diesem Zeitpunkt sichergestellt. Die Durchführung von Operationen wurde zunächst auf notfällige Maßnahmen begrenzt, da die computergesteuerte Zentralsterilisation nicht mehr funktionstüchtig war.

Beeinträchtigungen in der Radiologie

Primäre Zielsetzung in dieser Situation war die Aufrechterhaltung der hausinternen Kommunikation, die über Festnetz- und WLAN-Telefone, teils durch Läufer gewährleistet bleiben konnte. Im Weiteren wurde definiert, welche Funktionalitäten zur Verfügung standen. Abgesehen von der Laboratoriumsdiagnostik musste geklärt werden, welche Untersuchungen in der Radiologie unter den gegebenen Umständen noch durchgeführt werden konnten.

Da die Modalitäten primär im Hinblick auf die reine Bilderstellung nicht von einem Netzwerk oder zentralen Servern abhängig >

sind, ergaben sich prinzipiell keine Einschränkungen hinsichtlich des Untersuchungsumfangs. Allerdings waren wesentliche Voraussetzungen wie z.B. die Steuerung über digitalen Datenaustausch mit dem Radiologie-Informations-System (RIS) nicht mehr gegeben. Die Röntgenanforderungen mussten ab sofort handschriftlich auf Anforderungsformularen eingereicht werden. Die Untersuchungen wurden nach individuellem Abgleich der personenbezogenen Daten mit den Patienten direkt an der Modalität manuell angelegt. Es gab keine elektronische Dokumentation der erbrachten Leistungen und aller weiteren damit verbundenen Daten. Sämtliche Informationen wie auch die Dokumentation der nach Röntgenverordnung notwendigen Daten u.a. im Hinblick auf die Strahlenexposition mussten handschriftlich auf dem Anforderungsformular notiert werden. Die Befundmitteilung erfolgte telefonisch bzw. direkt mündlich, eine handschriftliche Dokumentation erfolgte in Kurzform ebenfalls auf dem Anforderungsformular. Diese wurden gesammelt, um für die spätere Nacherfassung zur Verfügung zu stehen.

Der Transfer in das elektronische Bildarchiv (PACS) war unterbrochen, die Speicherung der Daten musste also primär auf den Modalitäten erfolgen. Ebenso konnte eine externe Datensicherung über CD oder angeschlossene Laufwerke nicht erfolgen, da die Brennsoftware zentral aus dem PACS anzusteuern ist. Eine externe lokale Datenspeicherung war an den Modalitäten nicht etabliert. Ein Ausdruck auf Film war nicht möglich, da der Trockenlaser nur über das Netzwerk anzusteuern war. Eine direkte Überprüfung ergab, dass der zur Verfügung stehende Speicherplatz unter Beibehaltung der üblichen Untersuchungsfrequenzen im konventionellen Röntgen für ca. 14 Tage, am MRT für ca. zehn Tage und an den CT-Geräten für ca. eine Woche ausreichend gewesen wäre.

»Primäre Zielsetzung in dieser Situation war die Aufrechterhaltung der hausinternen Kommunikation.«

Die Röntgenaufnahmen und Schichtbilder konnten nur direkt an den Modalitäten betrachtet werden. Insbesondere für die konventionellen Röntgenbilder standen keine abgenommenen Diagnosemonitore zur Verfügung. Voraufnahmen lagen naturgemäß nicht vor, sodass Verlaufskontrollen nicht beurteilt werden konnten. Im Einzelfall wurden Bilder oder Bildserien beim Durchscrollen anonymisiert mit mobilen Devices (z.B. iPads, die üblicherweise für die mobile Visite verwendet werden) fotografiert oder gefilmt, um beispielsweise im OP betrachtet werden zu können.

Die Beeinträchtigungen in weiterer Hinsicht mögen durch die beiden folgenden Beispiele illustriert werden: Während des Systemausfalls stand nur etwa ein Drittel des üblichen Umfangs der Laboratoriumsdiagnostik zur Verfügung, die Eingangs-Befund-Laufzeit hatte sich aufgrund der auch dort notwendigen manuellen Erfassung von den üblichen etwa 30 Minuten auf mehrere Stunden verlängert. Es standen die für die Radiologie notwendigen Grundwerte zur Verfügung, jedoch nur auf handschriftlichen Befunden, die an die Stationen weitergereicht wurden, sodass ein erhöhter Kommunikationsaufwand mit verlängerter Latenz erforderlich war.

Der Hol- und Bringedienst wurde vom dynamischen PC-basierten auf ein stationsbasiertes System umgestellt. Pro Station stand ein Mitarbeiter zur Verfügung, der über Handy erreichbar war. So konnte die Aufrechterhaltung der Patientenverbringung gewährleistet werden, die aber nicht mehr bedarfsgesteuert werden konnte.

Schadenseinschätzung

Die zentralen Systeme der Radiologie wurden von Experten der RIS- und PACS-Hersteller nach Freigabe durch die IT isoliert zunächst hochgefahren und auf Schäden geprüft. Entscheidend hierbei war das letzte Server-Back-up, das wenige Stunden vor dem Herunterfahren abgelegt worden war. Ein Verlust im Hinblick auf Patientendaten bzw. Bilder konnte nicht festgestellt werden. Während zentral durch die IT sowie die externen Dienstleister die Server überprüft und langsam revitalisiert wurden, mussten in der Radiologie alle PCs und Workstations neu aufgesetzt werden, da sie durch die Schadsoftware befallen waren. Die Hersteller überprüften die Steuerrechner der Modalitäten proaktiv, es wurden jedoch zu keinem Zeitpunkt der Krise Einschränkungen in der

Funktionalität der Geräte festgestellt. Eine Erklärung könnte die Verwendung von sogenannten „Whitelists“ sein, die die Ausführung nur von dezidierten, für die Nutzung der Modalitäten erforderlichen Dateitypen und Programmen erlauben.

Die Kern-Funktionalitäten des RIS (Datenintegration, Dokumentation, Befunden, Spracherkennung) und des PACS (RIS-PACS-Kopplung, Bildverteilung ohne Anbindung an das Krankenhausinformationssystem (KIS)) standen in wesentlichen Teilen nach circa zehn Tagen wieder zur Verfügung. Die vollumfängliche RIS-PACS-KIS-Integration konnte nach etwa drei Wochen wiederhergestellt werden. Erst in dieser Phase konnte die nachgelagerte Dokumentation der Leistungen erfolgen, deren Voraussetzung allerdings die vollständige Erfassung des jeweiligen Patienten im zentralen KIS war. Der Gesamtaufwand für die Wiederherstellung allein der Radiologie-Systeme sowie der nachgelagerten Dateneingabe bzw. -korrektur ist mit insgesamt fünf bis sechs Mannwochen zu veranschlagen. Die Gesamtkosten des IT-Ausfalls dürften im hohen sechsstelligen Bereich gelegen haben.

Ursachenanalyse

Aufgrund der potenziell kriminellen Hintergründe wurden das Landeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik (BSI) frühzeitig durch die Geschäftsführung eingeschaltet. Beide Institutionen haben mit auch hohem personellem Aufwand zunächst versucht, unter dem Primat der Wiederherstellung der Sicherheit und der Vermeidung jeglicher Datenverluste die Ursache der Krise herauszufiltern. Der Arbeit dieser beiden Institutionen ist zu verdanken, dass eine Signatur der Schadsoftware und der wahrscheinliche Eindring-Mechanismus – am ehesten über aktives Umgehen der intakten Firewall – geklärt werden konnten, der dann neben der Neuentwicklung eines Virenscanners in eine Neugestaltung der IT-Landschaft mündete. Unter anderem wurde neben einer Erweiterung der Firewall durch Sandboxing sowie Network Access Control das bestehende Netzwerk segmentiert. Darüber hinaus wurde ein internes Whitelisting eingeführt.

Chancen aus der Krise

Abgesehen von der in dieser Krise optimalen Kooperation der einzelnen Abteilungen im medizinischen und nicht-medizinischen Bereich war ein positiver Effekt, dass die durch die ungewöhnliche Situation erhöhte Aufmerksamkeit zu weniger leichten Fehlern, u.a. auch in der Radiologie, führte. Später sollte sich herausstellen, dass die Erlössituation in der Phase der IT-Krise eher noch auf einem höheren Niveau als in den Vorjahren lag. Letztlich wurde die Situation genutzt, um eine noch modernere IT-Landschaft mit hohem Anspruch an externe und interne Sicherheitskriterien im laufenden Betrieb zu etablieren. ■

PROF. DR. MED. MATHIAS COHNEN

ist Chefarzt am Institut für klinische Radiologie der Städtischen Kliniken Neuss – Lukaskrankenhaus – GmbH

© UKSH GESELLSCHAFT FÜR IT SERVICES MBH

Abbildung 1:
Blick in einen Kaltgang eines TIER-III-Rechenzentrums

IT-Sicherheit und der FAKTOR MENSCH

Das Gesundheitswesen zählt zu den meistbedrohten Sektoren von Cyberkriminalität und die Angriffe auf die IT-Infrastrukturen von Kliniken nehmen zu. Doch was gilt es zu tun, um dort IT-Sicherheit zu gewährleisten? Ein ausführlicher Überblick.

TEXT: ARMIN WILL

Angriffe auf IT-Infrastrukturen im Gesundheitswesen werden immer häufiger.[1] Erstens weil die Infrastruktur möglichst frei zugänglich sein soll (Lieferanten- und Dienstleister-Wartungszugänge, Patiententerminals etc.), zweitens weil Angriffe mit vergleichsweise geringem Aufwand übers Internet möglich und weitestgehend anonym sind. Andererseits ist die Dienstleistung Krankenhaus nahezu vollständig von funktionierender IT-Infrastruktur abhängig. Maßnahmen zur Absicherung der Infrastrukturen sind daher zwingend.

Um die Wirksamkeit getroffener Schutzmaßnahmen an bereits identifizierten bzw. potenziell noch nicht bekannten Schwachstellen zu verifizieren, sind Penetrationstests eine etablierte Methode. Hierbei wird die IT-Infrastruktur auf Verwundbarkeiten überprüft und bewertet. Penetration Testing wird durch sogenannte Pen-Tester, die im Auftrag des IT-Infrastruktur-Betreibers versuchen, im laufenden Betrieb in die Computersysteme einzudringen, umgesetzt. Gelingt dies dem Pen-Tester, wird ein System bzw. die entsprechende Infrastrukturkomponente als unsicher eingestuft und es sollten umgehend geeignete und angemessene Maßnahmen eingeleitet werden, um das Gesamtsystem auf ein neues Sicherheitsniveau zu bringen. Eine Wiederholung des Tests dient der Validierung der getroffenen Maßnahmen.

Unberücksichtigt bei diesen Tests bleibt der Einfluss des Mitarbeiters, der mit den IT-Komponenten interagiert. Der Faktor Mensch und sein individuelles IT-Sicherheitsbewusstsein können mit technischen Penetrationstest nicht erfasst oder bewertet werden. Gerade aber das IT-Sicherheitsbewusstsein jedes Anwenders trägt, gegebenenfalls sogar entscheidend, zur IT-Sicherheit des Gesamtsystems bei. Unzureichendes Wissen um die eingesetzte Technologie, mögliche Gefahren und resultierende Folgeschäden bei IT-Infrastruktur-Anwendern stellen ein Risiko für die IT-Sicherheit dar. Dieses mangelnde IT-Sicherheitsbewusstsein machen sich Angreifer, zunehmend gezielt, zunutze. Trojanische Pferde und Social Engineering – insbesondere Phishing – sind prominente Beispiele, wie mangelhaftes IT-Sicherheitsbewusstsein eines Benutzers spezifisch ausgenutzt wird.

Bereits 2011 hat die Bundesregierung unter Federführung des Bundesinnenministeriums die Cybersicherheitsstrategie für Deutschland beschlossen.[2] In der Folge wurden etliche Maßnahmen zur Umsetzung der Strategie initiiert. Unter anderem wurden in neun Sektoren Kritische Infrastrukturen identifiziert, die sich durch das IT-Sicherheitsgesetz seit Dezember 2014 mit konkreten Anforderungen konfrontiert sehen.[3] Für einige Sektoren liegen die Kriterien zur Zuordnung von Betreibern zu den KRITIS vor, für den Sektor Gesundheit werden diese Kriterien aktuell definiert. Auch wenn bis zum Ende des Jahres nicht jedes Krankenhaus als KRITIS eingestuft wird: IT-Sicherheit gilt für alle.

Mit dem Förderprogramm „IT-Sicherheit für Kritische Infrastrukturen“[4] des Bundesministeriums für Bildung und Forschung (BMBF) werden gezielt sektorspezifische Anforderungen identifiziert, technische und organisatorische Konzepte entwickelt, um Kritische Infrastrukturen gegen Cybergefahren abzusichern.

Mit dem BMBF-Projekt ITS.APT (IT-Security Awareness Penetration Testing) wird am Universitätsklinikum Schleswig-Holstein (UKSH) der Fokus auf den Faktor Mensch als potenzielle Schwachstelle der IT-Infrastruktur gelenkt. Sowohl das Erfassen der individuellen IT-Security-Awareness wie auch – auf Basis der erhobenen Informationen gezielt zu fokussierende – Schulungen zur Stärkung des IT-Sicherheitsbewusstseins sowie anschließende Validierung der Schulungsmaßnahmen erfolgen im Rahmen von ITS.APT am UKSH.

»Der Faktor Mensch und sein individuelles Sicherheitsbewusstsein können mit einem technischen Penetrationstest nicht erfasst werden.«

Strukturen und Werkzeuge

Unternehmen der Gesundheitsbranche stützen sich bei der Erfüllung ihrer Kernaufgaben auf eine umfangreiche IT-Organisation und -Infrastruktur. Jedes Krankenhaus setzt dabei unterschiedliche Schwerpunkte und skaliert die IT-Strukturen entsprechend der Erfordernisse. In Grundzügen sind die nachfolgend skizzierten Elemente für ein funktionierendes Krankenhaus heute unverzichtbar. >

Kern einer funktionierenden IT-Infrastruktur sind Mitarbeiter. Ob diese nun durch das Krankenhaus selbst oder – wie zunehmend zu beobachten – von einer IT-Servicegesellschaft bereitgestellt werden, ist unerheblich. Entscheidend ist die Fachkompetenz der Mitarbeiter. Der Betrieb von Servern und Netzwerk, das Management von PC, Notebooks und mobilen Devices gehört in die Hände von Profis. Die Zeiten, als der Assistenzarzt der Fachabteilung den lokalen Server mal eben noch betreute, sind definitiv vorbei. Ein sicherer und verlässlicher IT-Einsatz über 24 Stunden am Tag an sieben Tagen in der Woche (24/7-Betrieb) muss an einem Krankenhaus (zumindest für die Kernsysteme) gewährleistet werden. Der kontinuierliche Betrieb der Systeme ist von kontinuierlicher Ausweitung der Anforderungen aus den klinischen und administrativen Bereichen flankiert. Immer umfangreicher sollen Daten erfasst und verarbeitet werden, Prozesse in einzelnen Bereichen, und übergreifend digital unterstützt werden. Insofern sind IT-Systeme in Krankenhäusern dynamische Systeme, die einem stetigen Weiterentwicklungsprozess unterliegen.

»IT-Systeme in Krankenhäusern sind dynamische Systeme, die einem stetigen Weiterentwicklungsprozess unterliegen.«

Die Anforderungen an Klinikrechenzentren sind nicht zu unterschätzen. Einerseits ist Ausfallsicherheit für den 24/7-Betrieb – zumindest für patientenkritische Systeme – sicherzustellen, andererseits eine recht große Skalierbarkeit einzuplanen, da mit zunehmender Laufzeit der Systeme sowohl Rechenleistung als auch Speicherplatzbedarf wachsen.

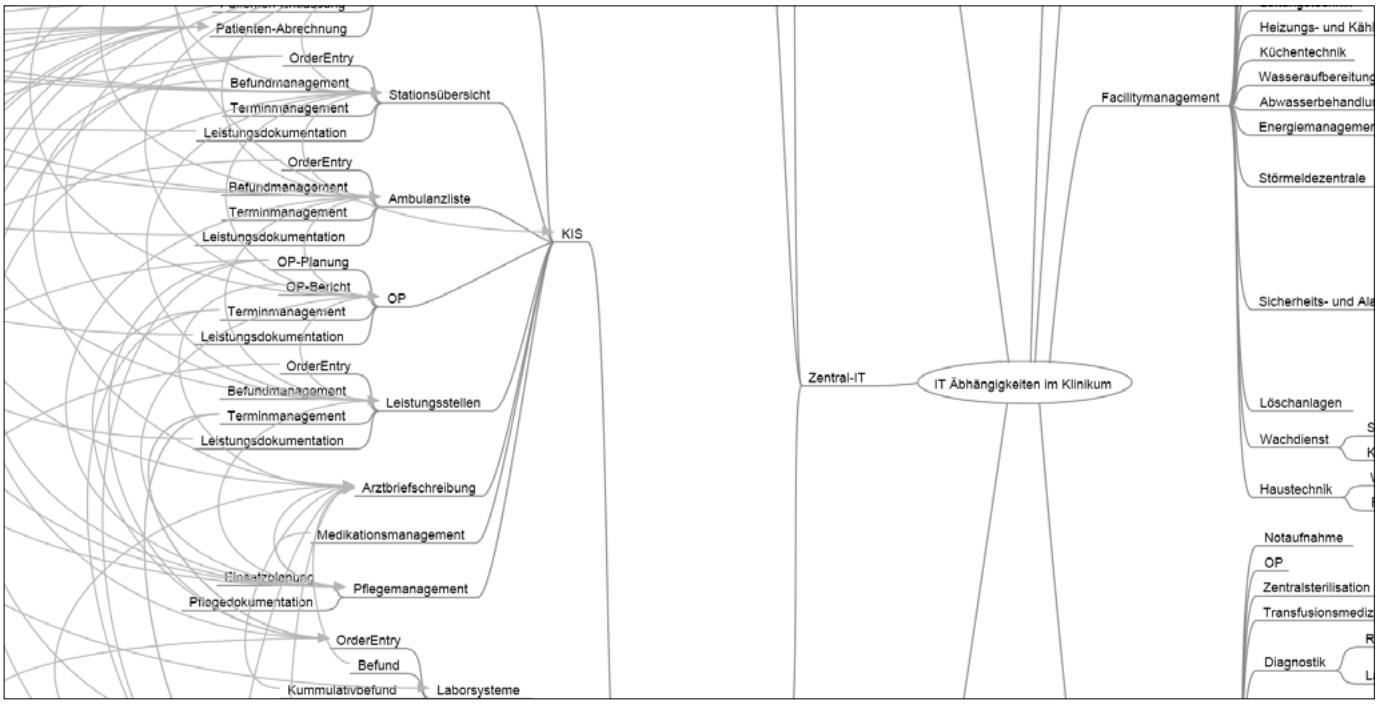
Ausfallsicherheit wird durch redundante Strukturen eines Rechenzentrums (RZ) erreicht. Mindestens zwei Serverräume in zwei unterschiedlichen Brandabschnitten sind idealerweise mittels redundanter Strom- und Klima-Installationen versorgt und über redundante Datenverbindungen gekoppelt. Unterbrechungsfreie Stromversorgung und gegebenenfalls eine eigene Notstromanlage sorgen für sichere Energiezufuhr. Umfassende Brandmelde-, Rauchabzugs- und Einbruchmeldeanlagen sowie gegebenenfalls erweiterter Hochwasserschutz ergänzen die strukturellen Sicherungsmaßnahmen für ein klinisches RZ. Ausfälle der Klinik-IT durch Störungen oder notwendige Wartungsarbeiten werden unter diesen Bedingungen weitestgehend vermieden, die Verfügbarkeit liegt bei 99,98 Prozent und Klinikbetreiber sollten für ihre Klinik-IT die Nutzung eines solchen TIER-III-Rechenzentrums anstreben.

Ein geflügeltes Wort in der Klinik-IT lautet „Storage ist nie genug da“. Insbesondere durch, im Vergleich zu anderen Bereichen, deutlich längere – für klinische Dokumente bis zu 30 Jahre – Aufbewahrungsfristen werden an die (Langzeit-)Speicher eines Klinik-RZ hohe Anforderungen gestellt. Ein abgestuftes Konzept umfasst neben einem zentralen Speichernetzwerk (Storage-Area-Network, SAN), verschiedene Network Attached Storage (NAS)-Systeme, revisionssichere Langzeitspeicher und kontinuierliche Back-ups. Das zu managende Storagevolumen eines Klinikums in der Größe des UKSH kommt schnell in PByte-Bereiche.

Neben der zentralen RZ-Struktur können im Einzelfall dezentrale Serverkomponenten notwendig sein, insbesondere bei daten- und kommunikationsintensiven Applikationen. In der Radiologie stellen z.B. MRT- und Röntgen-Serien enorme Anforderungen an die Netzwerk-Übertragungskapazität. Bei ausschließlich zentraler Speicherung kommt es gegebenenfalls schnell zu Engpässen. Ein dedizierter Server mit Kurzzeitspeicher (bis zu sechs Monate haben sich bewährt) kann die Latenzprobleme beim Aufruf der großen Datenmenge abfedern.

Neben zentralen Komponenten ist, je nach baulicher Struktur der Klinik unterschiedlich umfangreich ausgeprägt, eine – möglichst „alle Ecken“ abdeckende – Netzwerkinfrastruktur mit Router, Switches, Firewalls, Access-Points etc. durch die IT des Krankenhauses zu betreiben. Besonderes Augenmerk gilt dabei den Bereichen der Klinik, wo neben der „normalen“ Klinik-IT auch Geräte und Systeme aus dem Geltungsbereich der Medizinprodukte-Betreiberverordnung (MPBetreibV) in die Netzstruktur eingebunden werden. Hier sind durch die DIN EN 80001-1 besondere Sicherungsmaßnahmen notwendig. Eine enge Abstimmung mit der Medizintechnik ist zwingend.

Kostengünstig und am besten skalierbar hat sich Virtualisierung



© STABSSTELLE IT DES UKSH

Abbildung 2: *Ausschnitt aus dem Beziehungsgeflecht einer Krankenhaus-IT-Landschaft*

im Serverbereich inzwischen durchgesetzt, sodass im Allgemeinen die meisten Server als virtualisierte Server zentral gehostet werden. Ausnahmen stellen solche Geräte dar, bei denen spezifische, zwingend vorausgesetzte Hardwarekomponenten nicht transparent einer virtuellen Instanz zugewiesen werden können.

Schließlich muss die IT eines Krankenhauses auch die Endgeräte (Stationsarbeitsplätze) bis hin zu Geräten am Point-of-Care (POC), z.B. mobile Endgeräte, bereitstellen. Auch hierbei kann Virtualisierung die Anforderungen an die Endgeräte minimieren.

Wesentliche Anwendung eines Krankenhauses ist das zentrale Krankenhausinformationssystem (KIS). In der Kernarbeitszeit registriert das UKSH mehr als 3 000 parallele Sessions. Eine weitere wesentliche Komponente für den Krankenhausbetrieb ist das zentrale Enterprise-Resource-Planning (ERP). Der gesamte administrative Workflow außerhalb der Patientenversorgung wird hier abgewickelt. Es gibt Komplettlösungen, die sowohl klinische als auch administrative Prozesse abbilden. Selbst die größten Komplettpakete sind nicht in der Lage, alle – vor allem klinische – Anforderungen abzubilden. In vielen Kliniken, Ambulanzen und Instituten kommen daher spezifische klinische und administrative Spezialsysteme zum Einsatz, unter anderem Laborsysteme und klinische Fachsysteme. Sofern möglich werden diese auf zentralen Servern gehostet. In Ausnahmefällen müssen allerdings lokale Server betrieben werden.

Je größer die Zahl der notwendigen Systeme ist, desto komplexer wird die Vernetzung der Systeme untereinander. Grundsätzlich ist die direkte Anbindung einzelner Systeme untereinander möglich, aber irgendwann nicht mehr mit vertretbarem Aufwand zu betreuen. Der Einsatz eines zentralen Kommunikationsservers und die Nutzung gemeinsamer Verzeichnisdienste ermöglicht umfassenden Datenaustausch zwischen vernetzten Systemen unter bestmöglicher Datensparsamkeit und -sicherheit.

Digitalisierung

Daten, sowohl administrativ als auch klinisch, sind zunehmend digital. Industrie 4.0, Buzzword der industriellen Produktion, greift in gleicher Weise – vielleicht noch tiefgehender – in der Gesundheitsbranche in vorhandene Prozesse ein und generiert neue, bisher nicht notwendige Arbeitsabläufe. Neben Patientendaten, Untersuchungs- und Therapiedaten sind Behandlungspfade und Workflows digital abgebildet oder zur Einsicht hinterlegt. In ausgewählten Bereichen ist bereits seit Längerem Prozesssteuerung implementiert (z.B. Laborstraßen, Sterilisation, Essensversorgung). Auch unmittelbar die Patientenversorgung betreffende Prozesssteuerung hält zunehmend Einzug in Kliniken. Kommissionierungsautomaten bereiten die Medikation jedes einzelnen Patienten tagesaktuell, vollautomatisch auf. Einsatzplanung von Personal und das Management der Materialflüsse, die Belegung der Operationseinheiten sowie die Einsatzplanung der diagnostischen Einrichtungen erfolgen digital.

>

»Zu den „Basisrisiken“ gesellen sich zunehmend Risiken aus Vernetzung und Digitalisierung.«

Die Werkzeuge sind nicht nur zunehmend IT-gestützt, sondern zunehmend untereinander vernetzt. Mit mobilen Endgeräten erfasste Vitalparameter werden über Schnittstellen in der zentralen, elektronischen Krankenakte dokumentiert. Die mobil erfassten Materialverbräuche finden Eingang in die Krankenakte und lösen in der Materialverwaltung entsprechende Verbuchungen, bei Bedarf automatisierte Nachbestellungen bei Hersteller bzw. Lieferant aus. Mit der Online-Buchung einer Untersuchung oder Operation werden relevante Patienteninformationen (z.B. Allergien, Risikofaktoren, wesentliche Medikationen) übermittelt. Untersucher und Behandler stehen die Informationen der elektronischen Krankenakte unmittelbar am Behandlungsgerät zur Verfügung.

Ziel der Digitalisierung und Vernetzung ist die Optimierung der Behandlung des Patienten. Die transparente Bereitstellung notwendiger klinischer Daten am Ort des Geschehens sichert einen konsistenten Informationsstand. Die Verbesserung des Behandlungsworkflows durch IT-Einsatz kommt primär der Verbesserung der Behandlung des Einzelnen sowie dem beteiligten Mitarbeiter durch optimierte Arbeitsabläufe zugute. Unnötige Aktensuche, fehlende Informationen, Reduzierung des administrativen Aufwands ohne unmittelbaren Bezug zum Patienten helfen den Mitarbeitern, sich auf den Patienten zu konzentrieren.

Mit der Digitalisierung geht aber eine steigende Abhängigkeit von der digitalen Infrastruktur einher. Der Ausfall oder die Störung wesentlicher Komponenten der IT-Infrastruktur können erhebliche Auswirkungen – für Patienten eventuell letale Komplikationen – zur Folge haben. An einer Stelle falsch erfasste Informationen sind an allen anderen Stellen ebenfalls falsch und können fatale Folgen nach sich ziehen.

Mit steigender Komplexität der Vernetzung von Systemen und Daten gehen für den einzelnen Mitarbeiter Verständnis und Übersicht für Zusammenhänge verloren. Die Anteile einer Prozesskette und ihre Abhängigkeiten untereinander sind dem Einzelnen häufig nicht mehr transparent. Noch mehr geht das Verständnis und die Übersicht verloren, wenn verschiedene Prozessketten untereinander in Abhängigkeit stehen.

Dabei endet die Vernetzung bekanntermaßen nicht an der Krankenhausgrenze. Die Kommunikation mit den Kostenträgern, niedergelassenen Ärzten, Nachbehandlungseinrichtungen, Konsiliarii und zunehmend mit den Patienten selber, wird immer umfangreicher. Dabei werden die übertragenen Daten komplexer und sensibler (Datenschutz). Zu Wartungs- und Servicezwecken wird von Herstellern und Dienstleistern ein externer Zugang zur Krankenhaus-IT-Infrastruktur erwünscht, gefordert bzw. vorausgesetzt.

Im Ganzen ergibt sich ein nahezu unüberschaubares Geflecht von Beziehungen und Abhängigkeiten. Abbildung 2 gibt einen stark reduzierten Ausschnitt einer „Netzkarte“ einer Krankenhaus-IT-Landschaft wieder.

Bedrohungslage

Das komplexe System Krankenhaus braucht verlässliche Verfahren und Methoden zur Sicherung der Betriebsbereitschaft seiner IT-Infrastruktur und damit seiner Leistungsfähigkeit.

Verschiedenste Einflüsse können die Betriebsbereitschaft der IT-Infrastruktur gefährden: Stromausfall, Verbindungsstörungen / Unterbrechungen, Fehlfunktionen, Programmierfehler. Diesen „Basisrisiken“ kann mit bewährten Gegenmaßnahmen entgegengetreten bzw. vorgebeugt werden. TIER III RZ können mit entsprechender Notstromversorgung und redundanten Anbindungen Betriebsbereitschaftszeiten von 99,98 Prozent erzielen. Fehlfunktionen und Fehlbedienung kann durch Schulungen gezielt entgegengewirkt werden, Programmierfehler sind zwar nicht vermeidbar, können aber mit einem konsequenten Qualitätsmanagement bereits bei der Konzeption reduziert werden.

Doch wie sieht es mit Risiken aus, die sich durch die notwendige Vernetzung der IT-Infrastruktur mit dem Internet, mit Herstellern, Lieferanten etc. ergeben? Wie steht es mit Risiken bei Nutzung von Datenträgern mit Patienteninformationen, von Kollegen zugesandt oder vom Patienten mitgebracht?

Zu den Basisrisiken gesellen sich zunehmend Risiken aus Vernetzung und Digitalisierung. Was bedeutet Cyberkriminalität für die Krankenhaus-IT?

Für Angriffe auf die IT-Infrastrukturen im Gesundheitswesen sind die Voraussetzungen nahezu ideal. Fast ausnahmslos sind die Protagonisten der Gesundheitsversorgung gezwungen, elektronisch erreichbar zu sein. Seit Jahren erfolgt die Abrechnung

von Krankenhausleistungen vollständig per elektronischem Datenaustausch (§ 301). Zunehmend erwarten Dienstleister und Lieferanten Zugriff auf die von ihnen gelieferten Systeme zu Wartungs- und Servicezwecken, teilweise wird in Wartungsverträge freier Zugang gefordert, oder verlangt, dass Systeme „nach Hause telefonieren“ bzw. Daten in die Cloud laden können. Zudem haben Krankenhäuser unter permanentem Konkurrenzdruck ein großes Interesse, in der Öffentlichkeit wahrgenommen zu werden, ihren Patienten Informationen über die angebotenen Dienstleistungen zur Verfügung zu stellen und betreiben umfangreiche Internetpräsenzen und Patientenportale. Solche Schnittstellen sind zwangsläufig nach außen, oft direkt im Internet, exponiert.

Der Aufwand für einen Cyberangriff über das Internet ist überschaubar. In einschlägigen Kreisen werden fertige Toolboxen für die Erstellung von Cyberangriffen angeboten. Im sogenannten Darknet können spezifisch angepasste Angriffe als Dienstleistung gebucht werden.[5] Angreifer bleiben dabei weitestgehend anonym. Im Vergleich zu physischen Angriffen vor Ort kann der Angreifer seine Identität über das Medium Internet leichter verschleiern. Ob Angriffe gezielt, seit 2015 zunehmend zu beobachten, oder im Rahmen massenhafter Cyberattacken erfolgen: Krankenhäuser müssen – im eigenen Interesse, vor allem zum Schutz ihrer Patienten – Vorkehrungen gegen durch Cyberattacken verursachte Systemausfälle treffen. Hierbei scheint Deutschland ein besonders lukratives Ziel zu sein. Laut einer aktuellen Studie des Kaspersky Lab stand Deutschland im Zeitraum zwischen April 2015 und März 2016 am stärksten unter Beschuss. So stieg der Anteil der angegriffenen Anwender um 35,65 Prozent gegenüber dem Vergleichszeitraum 2014-2015.[6] Zudem verdoppelte sich der Anteil der Attacken auf Unternehmen von 6,8 Prozent auf 13,13 Prozent.[7]

Obwohl die Schlagzeilen produzierende Ransomware Krankenhäuser nicht gezielt attackierte, muss doch konstatiert werden, dass 2015 >

ANZEIGE

imprivata®

The healthcare IT security company

Imprivata Lösungen

- Schützen und beschleuningen den Zugriff auf Patientendaten
- Single Sign-On und schneller Zugriff auf virtuelle Desktops
- Zwei-Faktor-Authentifizierung für klinische Arbeitsabläufe
- Identitätsmanagement und Authentifizierung

Fordern Sie weitere Informationen an und schreiben Sie uns an info @ imprivata.de oder besuchen Sie www.imprivata.de um unser Paper zu den aktuellen gesetzlichen Vorgaben für die Krankenhaus-IT herunterzuladen.
Tel: 0911-8819 7330

die Zahl an Cyberangriffen auf das Gesundheitswesen gegenüber 2014 deutlich zugenommen hat. Hintergrund ist, dass medizinische Daten für Angreifer lukrativer sind als z.B. Kreditkartendaten. Während kompromittierte Kreditkartendaten schnell und effizient „neutralisiert" werden können, sind medizinische Informationen von Patienten meist permanent und in vielen Fällen nur schwer bzw. mit hohem Aufwand wiederherzustellen. Laut dem IBM X-Force Threat Intelligence Report 2016 müssen betroffene Organisationen für jeden kompromittierten Patientendatensatz 363 US-Dollar aufwenden, während durchschnittlich andere Arten von Datensätzen lediglich Kosten in Höhe von 154 US-Dollar nach sich ziehen. Dies spiegelt sich auch beim illegalen Handel gestohlener Daten wider: Während abgefischte Kreditkartennummern zu Schleuderpreisen verramscht werden, werden für gestohlene Patientendaten bis zu 50 US-Dollar pro Datensatz aufgerufen. Der Cybercrime-Markt orientiert sich um. Allein in den USA sind nach einer Studie des Ponemon Institute[8] Einrichtungen des Gesundheitswesens im Schnitt einmal pro Monat einer Cyberattacke ausgesetzt. Dabei geht es (noch) vornehmlich um Datendiebstahl, aber die Tatsache, dass etliche patientenversorgende Systeme ungenügend gegen Attacken abgesichert sind, lässt befürchten, dass konkrete Angriffe auf Patienten, zumindest als Drohkulisse, interessant werden.

Am 25.02.2016 zitierte die Ärzte-Zeitung eine Untersuchung der Firma Gemalto.[9] Nach Analyse von 1 673 weltweiten öffentlich bekannt gewordenen Hackerangriffen wurden insgesamt über 700 Millionen Datensätze kompromittiert bzw. entwendet. Unternehmen des Gesundheitswesens waren zu 19 Prozent betroffen.

Auch wenn Krankenhäuser nicht gezielt Cyberattacken ausgesetzt sind, können bei einem erfolgreichen Angriff dennoch immense Kosten entstehen. So musste das Lukaskrankenhaus Neuss laut kma einen Schaden in Höhe von 1,7 Millionen Euro feststellen.[10] Auch wenn der Schaden durch das Nachholen der ausgefallenen Operationen auf rund 900 000 Euro reduziert werden konnte, wird doch deutlich: Erfolgreiche Cyberattacken verursachen immense Kosten. Solange bei Angriffen keine Patienten zu Schaden kommen, leidet die Reputation eines betroffenen Krankenhauses nur wenig, aber ausschließen, dass erfolgreiche Cyberangriffe zu Patientengefährdungen führen, kann niemand.

Schwachstellen

Vor dem Hintergrund dieser Bedrohungslage ist ein Krankenhaus gefordert, die Schwachstellen bei Betrieb und Nutzung von IT zu kennen und mit geeigneten Maßnahmen zu beheben bzw. abzusichern.

Nachfolgend sollen einige der bekanntesten potenziellen Schwachstellen betrachtet werden.

Organisation

Auch wenn das Krankenhaus seine IT nicht selbst betreibt, bleibt die Verantwortung für den Krankenhausbetrieb, gerade auch die Sicherstellung der Funktionsfähigkeit der IT als zentraler Komponente für die Erbringung der Dienstleistung Gesundheitsversorgung, in der Verantwortung der Geschäftsführung. Hat die Geschäftsführung jedoch keine IT-Sicherheitsziele definiert, sind die Verantwortlichen für Einhaltung und Erreichung der Ziele nicht klar bestimmt, liegt organisatorisches Versagen vor, das vor dem Hintergrund des IT-Sicherheitsgesetzes neben empfindlichen Bußgeldern auch Schadenersatzforderungen nach sich ziehen kann. Dementsprechend sollte die Geschäftsführung dafür sorgen, dass die zu beteiligenden Bereiche bzw. Personen mittels stringenter Prozessdefinitionen einerseits über eindeutige Verfahrensbeschreibungen und Handlungsanweisungen verfügen, andererseits die notwendigen Kompetenzen und Verantwortlichkeiten für alle transparent festgelegt sind. Ein dem wachsenden IT-Umfeld stetig anzupassendes Eskalations- und Risikomanagement sind zu etablieren und müssen Eingang in das Sicherheitskonzept finden. Nur bei gründlicher Analyse und Dokumentation können fehlende oder unzureichende Strukturen (Ansprechpartner und Zuständigkeiten, alternative Kommunikationswege, Vertretungsregelungen, Kompetenzlücken bzw. Konflikte, Eskalationspfade und Notfallpläne) identifiziert und zielgerichtet behoben werden.

Technik

Ein wesentlicher Teil bei Einführung und Durchführung eines IT-Sicherheitskonzeptes ist die ausführliche Bestandsaufnahme vorhandener Technik. Es ist erschreckend, wie viele veraltete, ungepatchte Systeme in Betrieb und vielfach auch im Netzwerk eingebunden sind. Die Gründe hierfür sind vielschichtig. Es gibt medizintechnische Systeme, die aufgrund von Zulassungsbestimmungen nicht ohne Weiteres mit einem Update versorgt werden dürfen. Wenn dies der Betreiber dennoch macht, riskiert er, das Gerät außerhalb der Zulassung zu betreiben und damit die vollständige

Verantwortung bei Fehlfunktion zu übernehmen, Stichwort Eigenherstellung. Neben veralteten Systemen (z.B. Windows XP) sind aber auch immer wieder fehlende Updates, nicht nur an PCs, anzutreffen, z.B. anfällige Firmware (z.B. Router). Weitere Schwachstellen werden durch fehlende Deinstallation nicht mehr genutzter Systeme und Programme eröffnet. Bei genutzten Programmen und Systemen sind immer wieder unzureichende Konfigurationen zu finden. Offene, nicht notwendige Ports, fehlender bzw. nicht aktueller Virenschutz, unregelmäßige und fehlende Firewall-Überprüfung und allzu oft einfache Adminpasswörter, unvollständige Rollen- und Profilzuordnung erleichtern Angreifern den Zutritt in IT-Systeme. Zudem ist die IT-Landschaft teilweise bereits so unübersichtlich, dass eventuell in dem einen oder anderen Büro ein seit Jahren zwar lokal genutzter, aber nicht gepflegter Server sein Dasein fristet. Aus der zunehmenden Digitalisierung der Prozesse ergibt sich eine erhöhte Komplexität der Vernetzung, mit neuen Wechselwirkungen und Abhängigkeiten. Multiple Komponenten mit unterschiedlichsten Sicherheitsmechanismen sind über mehrere Segmente miteinander vernetzt und es erfolgt häufig nur unzureichendes Monitoring genehmigter Zugriffe.

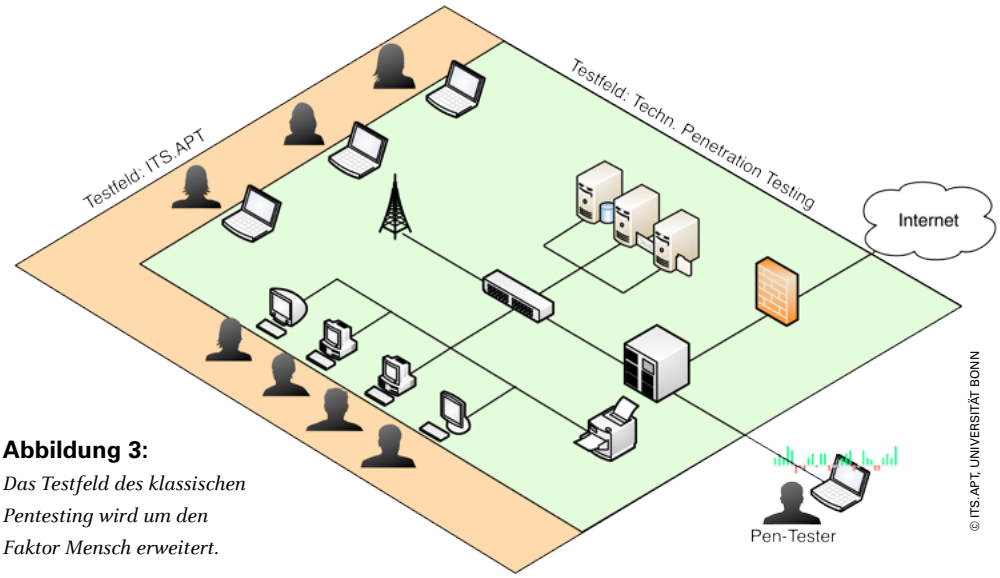


Abbildung 3:
Das Testfeld des klassischen Pentesting wird um den Faktor Mensch erweitert.

Mensch

Schließlich bleibt noch der vermeintlich größte Schwachpunkt bei der Einhaltung von IT-Sicherheit zu betrachten: die Schwachstelle Mensch.

Neben fehlendem Sicherheitsbewusstsein (Passwort unter der Tastatur, Zugangssharing, Verzicht auf Abmelden oder Sperren des Accounts) stellen das (blinde) Vertrauen in die Technik (Mail-Filter, Virenschutz, Firewall) und vor allem in die eigenen Fähigkeiten (Verzicht auf Verifikation, Verzicht auf regelmäßige Schulungen) häufig kritische IT-Sicherheitslücken dar.

Gezielt angegriffen werden menschliche „Schwächen“ wie Hilfsbereitschaft, Mitgefühl, Neugierde, Suche nach Anerkennung und Glück etc. Mittels gezielter Mails und Internetseiten erfolgt das sogenannte Social Engineering, um für den Zugriff auf IT-Systeme notwendige Information zu erhalten. Hier sollte sich jeder Anwender bewusst sein, dass er vor einer solchen Attacke nicht gefeit ist. Niemand sollte sich einbilden, für Angreifer kein lohnendes Opfer zu sein: Auch wenn „nur“ der Rechner des Pförtners kompromittiert wird, von dort in die gesamte IT-Landschaft ist es für einen Angreifer nur noch „ein Klick“.

Gegenmaßnahmen

Bei aller Bedrohung und bei allen bestehenden oder potenziellen Schwachstellen sind Krankenhäuser aber nicht hilflos.

In verschiedenen Gesetzen, Verordnungen, Normen und Empfehlungen sind für Krankenhäuser Rahmenanforderungen definiert und – teilweise zwingend, teilweise mit empfehlendem Charakter – zur Verwendung bereitgestellt. Orientiert sich ein Krankenhaus bei der Etablierung seines IT-Sicherheitskonzeptes an den Empfehlungen des BSI-Grundschutzes nach ISO 2700x, etabliert ein Risikomanagement angelehnt an den Leitfaden Risikoanalyse Krankenhaus-IT, setzt die Anforderungen der DIN EN 80001-1 in seinem IT-Netz um, sind bereits viele kritische Schwachstellen adressiert. Wenn zudem Hersteller ihre IT-Komponenten und Systeme vermehrt einer „Common Criteria for Information Technology Security Evaluation“ unterziehen und sich entsprechend zertifizieren lassen (Stichwort: Security by designe), kann weiterer Zugewinn an Cybersicherheit für die Betreiber dieser Komponenten gewonnen werden.

Der Einsatz von hochverfügbaren Komponenten, ein permanentes Monitoring des Systemzustands, regelmäßige Datensicherung und ausgefeilte Notfallpläne sind die Basis für den verantwortungsvollen Betrieb einer Krankenhaus-IT-Infrastruktur, eingebettet in ein effektives – möglichst schlankes – IT-Sicherheitskonzept. Den technischen Instrumentarien und organisatorischen >

»IT-Systeme in Krankenhäusern sind dynamische Systeme, die einem stetigen Weiterentwicklungsprozess unterliegen.«

Maßnahmen müssen zwingend Mitarbeiter mit notwendiger Kompetenz zugeordnet werden. Dabei stehen ebenfalls Normen bzw. Standards zur Qualifizierung und Zertifizierung der Mitarbeiter zur Verfügung (z.B. ITIL). Allerdings steht hier meist nur der technische Mitarbeiter im Fokus. Dieser ist zwar an zentraler Stelle wesentlich, aber – mit Blick auf Cybersicherheit – durchaus nicht allein entscheidend.

Entscheidend ist die Awareness des normalen Anwenders, seine Sensitivität gegenüber potenziellen Bedrohungen und Risiken. Das Bewusstsein der latenten Verwundbarkeit – gerade auch hinter der vermeintlich sicheren Firewall – ist zu schärfen, die Kenntnis über die aktuelle Bedrohungslage zu verbessern und bei jedem Anwender eine kontinuierliche Wachsamkeit zu erzeugen.

Vonseiten der Angreifer steht zunehmend der Mensch, als Anwender, im Fokus, da dieser die vermeintlich größte Schwachstelle des Systems darstellt.

Das Projekt ITS.APT

Gemeinsam mit Psychologen[11], Juristen[12], Datenschützern[13], einem IT-Sicherheitsdienstleister[14] und IT-Sicherheitsforschern[15] verfolgt das UKSH in dem vom BMBF geförderten Projekt ITS.APT drei Ziele. Es wird ein Testverfahren entwickelt, mit dessen Hilfe die IT-Security-Awareness von Anwendern ermittelt werden kann. Auf der Basis der Testergebnisse wird ein Schulungskonzept erstellt, welches die IT-Security-Awareness der Anwender verbessert und schließlich wird dieses Konzept am UKSH validiert.

Ausgangslage ist der klassische Pentest. Gute Pen-Tester unterziehen zunächst die getroffenen organisatorischen Maßnahmen einer differenzierten Prüfung und wenden sich anschließend der IT-Infrastruktur zu. Das Penetration Testing wird idealerweise durch externe Dienstleister vorgenommen, da es internen Überprüfungen häufig nicht gelingt, einen unabhängigen Blick „von außen“ zu bekommen. Die beim Pen-Test als unsicher eingestuften System- bzw. Infrastrukturkomponenten sollten umgehend mit angemessenen und geeigneten Maßnahmen auf ein höheres Sicherheitsniveau gebracht und das Ergebnis validiert werden.

Trotz aller technischen Raffinesse und persönlichen Erfahrung des Pen-Testers bleibt bei solchen Tests der Einfluss des mit den IT-Komponenten interagierenden Mitarbeiters unberücksichtigt. Das individuelle IT-Sicherheitsbewusstsein kann mit technischen Penetrationstests nicht erfasst oder bewertet werden. Das IT-Sicherheitsbewusstsein jedes Anwenders – nicht nur der IT-Mitarbeiter – trägt aber, ggf. sogar entscheidend, zur IT-Sicherheit des Gesamtsystems bei. Fehlendes Wissen über die eingesetzte Technologie, potentielle Gefahren und Folgeschäden stellen ein Risiko für die IT-Sicherheit dar.

Angreifer machen sich mangelndes IT-Sicherheitsbewusstsein auf vielfältige und differenzierte Weise zu Nutze. Bekannte Beispiele sind Trojanische Pferde und Social-Engineering – insbesondere Phishing – mit denen das mangelhaftes IT-Sicherheitsbewusstsein eines Benutzers gezielt ausgenutzt wird. Erstmals wissenschaftlich fundiert und abgesichert wird am UKSH mit ITS.APT der Fokus auf den Faktor Mensch als potentielle Schwachstelle der IT-Infrastruktur gelegt. Das Testfeld des klassischen Pentesting wird um den Faktor Mensch erweitert (Abbildung 3).

Auf der Basis einer fundierten Analyse bekannter Angriffsvektoren werden Artefakte identifiziert, die mit Angriffen einhergehen und durch Menschen wahrnehmbar sind. Ausgewählte Mitarbeiter werden mit diesen Artefakten während ihrer normalen Tätigkeit am PC konfrontiert und ihre Reaktion auf die Artefakte dokumentiert. Die Test-Teilnehmer werden anhand abstrakter Kriterien (Abteilung, Aufgabenbereich, Intensität der Computernutzung) ausgewählt, Reaktionsprotokolle nur anonymisiert bzw. pseudonymisiert erstellt. Die Ergebnisse lassen den Grad der Awareness ableiten und dienen der Konzeption gezielter Schulungsmaßnahmen zur Verbesserung der Awareness.

Die Beobachtung menschlichen Verhaltens mittels des skizzierten Testszenariums tangiert gleich mehrere gesetzlich geregelte Felder: Persönlichkeitsrecht, Arbeitsrecht, Haftungsrecht und den Datenschutz. Hier arbeitet das Projekt von Anfang an mit den lokalen Personalvertre-

tungen des UKSH und dem Datenschutzbeauftragten zusammen.

Fazit

IT-Sicherheit im Krankenhaus ist leistbar, auch wenn die Cyberkriminalität zunimmt. Organisatorische und technische Lösungen stehen zur Verfügung und müssen „nur noch" konsequent und effektiv im Tagesgeschäft umgesetzt werden. Dies erfordert zusätzliche Investitionen, einerseits in Technik, andererseits in Menschen. Krankenhausbudgets sehen derzeit hierfür keine Positionen vor. Hier bedarf es einer Anpassung der Krankenhausfinanzierung.

Nur qualifizierte Mitarbeiter sind in der Lage, die Konzepte und Techniken in der Praxis effektiv umzusetzen. Informierte und wachsame Mitarbeiter, mit geschulter Sensitivität für Risikosituationen und Bedrohungen durch Cyberangriffe können diesen angemessen begegnen. Das Bewusstsein einer latenten Bedrohungslage und Verwundbarkeit tragen wesentlich zur Sicherheit des gesamten IT-Systems bei. Der verantwortungsvolle Umgang mit IT-Komponenten unter kontinuierlicher Wachsamkeit jedes einzelnen Mitarbeiters können die Klinik-IT gegen Cyberangriffe härten. So werden informierte und sensibilisierte Mitarbeiter zur stärksten Waffe gegen Cyberangriffe und zu zentralen „Komponenten", um die Vulnerabilität einer IT-Infrastruktur zu verringern. ■

DR. ARMIN WILL

Stabsstelle Informationstechnologie
am Campus Lübeck des Universitätsklinikums Schleswig-Holstein

LITERATURVERZEICHNIS

1 Security Insider, Cyberkriminelle im Gesundheitswesen, 28.12.15 | Redakteur: Peter Schmitz, http://www.security-insider.de/cyberkriminelle-im-gesundheitswesen-a-516281/, zuletzt abgerufen: 07.01.2016

2 Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Innern, Alt-Moabit 101, D 10559 Berlin

3 Bundesministerium des Innern, IT und Cybersicherheit, https://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/it-cybersicherheit_node.html, zuletzt abgerufen: 15.09.2016

4 Bundesministerium für Bildung und Forschung, Bekanntmachungen, https://www.bmbf.de/foerderungen/bekanntmachung-878.html, zuletzt abgerufen: 05.09.2016

5 Heise Security, Ronald Eikenberg: Online-Dienst erstellt maßgeschneiderte Krypto-Trojaner, https://www.heise.de/security/meldung/Online-Dienst-erstellt-massgeschneiderte-Krypto-Trojaner-2668860.html, veröffentlicht: 27.05.2015 16:06 Uhr, zuletzt abgerufen: 12.09.2016

6 KSN Report: Ransomware in 2014-2016, Kaspersky-Labs, Moskau, Juni 2016

7 ebenda

8 Ponemon Institute, Dr. Larry Ponemon: Healthcare organizations are in the cross hairs of cyber attackers, https://www.ponemon.org/blog/healthcare-organizations-are-in-the-cross-hairs-of-cyber-attackers, veröffentlicht: February 29, 2016, 12:00 am, zuletzt abgerufen: 15.09.2016

9 Ärzte Zeitung, Marco Hübner: Gesundheitssektor ist häufig Ziel von Hackern, http://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/905822/studie-gesundheitssektor-haeufig-ziel-hackern.html?sh=5&h=-966258025, veröffentlicht: 25.02.2016 06:46 Uhr, zuletzt abgerufen: 15.09.2016

10 kma-online, 900.000 Euro Gesamtschaden durch Cyberattacke, https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durch-cyberattacke-a-31629, Quelle: Guntram Doelfs, veröffentlicht: 24.06.2016 12:22 Uhr, zuletzt abgerufen: 15.09.2016

11 Universität Duisburg-Essen, Fachgebiet Allgemeine Psychologie: Kognition

12 Universität Münster, Institut für Informations-, Telekommunikations- und Medienrecht

13 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

14 Enno Rey Netzwerke GmbH

15 Universität Bonn, Institut für Informatik 4: Arbeitsgruppe IT-Sicherheit

IT-Sicherheit im KRANKENHAUS

Anfang 2016 gab es eine Phase verhältnismäßig großer Unruhe in Deutschland und im Gesundheitswesen. Anlass war die umfangreiche Berichterstattung über erfolgte Cyberangriffe (auch) auf Krankenhäuser. Zeit für die Frage: Was bleibt nach ein paar Monaten?

TEXT: MICHAEL THOSS

Der Jahresbeginn war geprägt vom Eindruck massiver strategischer Angriffe auf Kliniken und deren Datenbestände. Neben dem Einsatz erpresserischer Trojaner mit Datenverschlüsselungsalgorithmen kamen auch andere Vorfälle zur Sprache. Besonders prägend war hierbei, dass einzelne Kliniken scheinbar in ihrer Infrastruktur so stark beeinträchtigt wurden, dass in Einzelfällen sogar die Leistungserbringung betroffen war. Ob dies tatsächlich ausschließlich dem Umstand des Cyberangriffs geschuldet war oder eventuell an begleitendem organisatorischen Versagen (Umsetzung von Notfallplänen) lag, konnte bisher nur in wenigen Fällen verbindlich geklärt werden. Thematisch ist dies ohnehin im Bereich der kontinuierlichen Verbesserungsprozesse zu sehen. Bei diesen sind mit absoluter Sicherheit entsprechende Effekte eingetreten. Allerdings müssen Alternativprozesse – für den Ausfall von elektronischen Datenverarbeitungsanlagen – zur Absicherung von Vorfällen sicherlich wieder mehr in den Fokus rücken. Notfallpläne betreffen nicht nur die IT, sondern im Wesentlichen diejenigen, die trotzdem weiterarbeiten müssen.

Panikmache versus Risikominderung

Gleichzeitig mit Vorfällen und Berichterstattung erfolgte eine schon fast systematische Panikmache, die unter anderem auch durch die Industrie getrieben wurde. Bei einigen Vertretern der Zunft konnte man den Eindruck gewinnen, dass Krankenhäuser über keinerlei Schutz und Technologien verfügen und jetzt unbedingt (noch mehr) technische Werkzeuge beschaffen müssten, um solche Probleme zukünftig zu verhindern. Was natürlich Unsinn ist. Weder treiben Krankenhäuser keinen Aufwand bei der Sicherheit noch würde das zukünftig Probleme wirklich vermeiden können. Es stellt sich sogar die Frage, ob sich die Quote der Betroffenen tatsächlich senken ließe, denn Art und Weise des nächsten Vorfalls sind nicht vorhersehbar.

Da es generell keinen hundertprozentigen Schutz gibt, kann man das technische Risiko bestenfalls vermindern. Das entspricht auch dem üblichen Vorgehen im Risikomanagement: vermeiden, vermindern, delegieren, akzeptieren. Die Frage ist, wofür man sich an welcher Stelle entscheidet und was als „Versicherungspolice“ wirtschaftlich vertretbar ist. Vermindern ebenso wie akzeptieren beinhaltet aber starke organisatorische Anteile. Man kann ja schlecht auf Technik als Ersatz für Technik setzen, die aktuell am Boden liegt. Der Einfluss auf die weichen Komponenten wie Personal ist dabei ungleich komplizierter, aber bedeutender Bestandteil jedes Szenarios. Sowohl zur präventiven Störungsvermeidung als auch bei der aktiven Störungsbewältigung.

Fakt sind zwei Dinge: Erstens ist statistisch nichts wirklich Außergewöhnliches passiert ist. Alleine, weil die Referenzwerte fehlen. Lediglich die Aufmerksamkeit hat durch Gesetzesinitiativen wie KRITIS und ITSiG zugenommen und folglich die Berichterstattung einen breiteren Raum eingenommen. Zweitens besteht das Bedrohungsszenario fort, es wird aber kaum noch darüber berichtet. Vermutlich weil es aktuell an Drama mangelt. Unabhängig von Dunkelziffern liegt aber die Summe der bekannten Vorfälle prinzipiell im zu erwartenden statistischen Rahmen. Ein Grund zur Panik oder kein Grund zur Panik? Panik ist sicherlich wenig hilfreich und folglich Besonnenheit das Mittel der Wahl.

»Weder treiben Krankenhäuser keinen Aufwand bei der Sicherheit noch würde das zukünftig Probleme wirklich vermeiden können.«

Was ist IT im Krankenhaus heute?

Beschäftigen wir uns heute mit IT im Krankenhaus, so muss der erste Schritt sein, den Begriff der „IT“ im Krankenhaus – oder allgemein – auch für den Laien richtig zu definieren. Klassische IT stellt dabei nur einen Teil des Versorgungsspektrums „IT“ dar. Daneben existiert das weite Feld der „IP“-basierten Technologien wie der Telekommunikation, der Fernsehversorgung, der Videoüberwachung oder der Gebäudeleittechnik (GLT). Gemeinhin sprachlich auch gerne als Internet der Dinge verklausuliert. Das große und mittlerweile längst bedeutendste Feld stellt allerdings im >

© MAKSIM KABAKOU – FOTOLIA

Krankenhaus die Medizintechnik dar. Diagnostische und therapeutische Systeme liefern heute in erheblichem Umfang Beiträge in die digitale Welt des Krankenhauses und sind somit Bestandteil der Vernetzung auf dem Weg zur digitalen Akte. Da hat es im Rahmen der Sicherheitsvorfälle schon den einen oder anderen verwundert, als – ganz kurz – die Äußerung eines Verbandssprechers in die Medien geriet, dass „die Sicherheit medizintechnischer Systeme in den Netzen schon Sache des Krankenhauses sei …". Schwierig, wenn viele Herstellersysteme selbst 2016 nicht dem aktuellen Stand der Technik entsprechen und teilweise nicht einmal Antivirenprogramme verkraften, ohne dass die Betriebserlaubnis infrage gestellt ist. Glücklicherweise hatte diese Position eine sehr kurze Lebenserwartung und wird sicherlich nicht in dieser Form wiederholt werden. Außer man strebt an, sich aus dem Markt zu diskutieren, denn die bestehenden und zukünftigen steigenden Sicherheitsanforderungen machen zwingend ein Umdenken bei der Industrie erforderlich.

Das letzte und schwierigste Feld des Risikomanagements stellt zweifellos das Personal dar. Erforderliche Mechanismen (schon befristete Passwörter), Regeln und Standards (Bildschirmschoner, Auto-Log-out) behindern aus dessen Sicht häufig die Arbeit, freie Datennutzung für freie Bürger ist ein Muss und die „Gleicher als Gleich"-Problematik bei Führungskräften führt ebenso häufig zur problematischen Durchsetzbarkeit erforderlicher Regelwerke. Egal ob bei Endgeräten oder der Nutzung von Medien wie Internet und E-Mail.

Was ist also zu tun?

Wichtige Schritte sind bereits eingeleitet und teilweise umgesetzt. Die DIN 80001 bietet bereits heute Möglichkeiten der Einflussnahme per Risikomanagement bei der Integration von medizintechnischen Systemen. In Verbindung mit einem Beschaffungs-Vetorecht der IT lässt sich auf diesem Wege Einfluss auf die Industrie nehmen und mittelfristig mehr Sicherheit erreichen. Das ITSiG wird dies noch unterstützen, da der IT-Sicherheitsbeauftragte unter dessen Rahmenbedingungen kein formaler Aspekt ist, sondern als Funktion mit weitreichenden Kompetenzen ausgestattet werden muss. Mal eben einen Beauftragten benennen, damit im Bericht der Wirtschaftsprüfer eine Fußnote entsteht, reicht in diesem Fall nicht aus.

Was ist bereits getan?

Man konnte in den vergangenen Monaten den Eindruck gewinnen, dass viele Industrievertreter ein Bild der Unterversorgung schüren wollten. Verständlich mit Blick auf erhoffte Zusatzumsätze, aber leider auch nicht so verantwortungsbewusst, wie man es wünschen würde. In kritischen Bereichen oder bei ermittelten Schwachstellen werden natürlich sinnvolle Diskussionen zum Ausbau von Schutzmechanismen geführt werden. Davon auszugehen, dass man alles neu machen muss, ist aber absurd. Tatsächlich verfügen alle Krankenhäuser über komplexe Schutzmechanismen. Dazu gehören Firewalls, Content- und Spamfilter, Antivirenprogramme auf mehreren Ebenen (zentral, dezentral), Sicherheitslösungen für IDS (Intrusion Detection System) oder andere Szenarien, Netzwerksicherheit, Fernwartungslösungen und vieles mehr. Da bleibt bestenfalls ein Delta für Optimierungen oder man gelangt schnell an den Punkt, wo zwar die Investition erbracht wird, der Nutzen aber kaum nachweisbar sein wird. Außer man argumentiert mit „Siehste, ist ja nichts passiert." Das kann aber auch andere Gründe haben. Daher gelten

© ARTEMSAM – FOTOLIA

die gleichen Anforderungen an das Risikomanagement wie vor den Vorfällen des aktuellen Jahres. Manche Regelungen des Datenaustauschs oder Kommunikationsverkehrs werden verschärft werden. Dafür ist der Boden sicherlich nun besser bereitet. Mit etwas Glück ist auch bei dem einen oder anderen Management eine Sensibilisierung eingetreten, die Auswirkungen auf dringend erforderliche Regelwerke und Budgets hat. Das große Geschäft wird das aber nicht auslösen, denn aufgrund der hohen Datenschutzauflagen im klinischen Umfeld sind die Standards ohnehin bereits sehr hoch.

Was kann man zusätzlich tun?

Die Ausbildung und Schulung der Mitarbeiter kann intensiviert werden, um deren Sensibilität zu schüren und die Sicherheitsregelwerke der Kliniken dürfen nicht einfach durch vermeintliche Unbequemlichkeiten ausgehöhlt werden. Neben technischen Angriffen ist immer noch Social Phishing eines der großen Risiken sowie das mangelnde Bewusstsein der Beschäftigten für die technischen Möglichkeiten von Angreifern. Dabei müssen sich die Angriffe nicht einmal direkt auf eine Einrichtung richten, es reicht mit ziemlicher Sicherheit schon, den E-Mail-Verkehr mitzuschneiden. Da werden sicherlich bei der Übermittlung zwischen Firmenaccount und privatem Account Dinge enthalten sein, die dort nicht hingehören. Eben weil es „bequem“ ist.

»Aufgrund der hohen Datenschutzauflagen im klinischen Umfeld sind die Standards ohnehin bereits sehr hoch.«

Darüber hinaus dürfen Notfallpläne nicht nur ein lokales Thema der IT sein und sich auf die Wiederherstellung von Systemen beziehen. Das ist zwar erforderlich, bei einem unvorhersehbaren Szenario lassen sich jedoch logischerweise keine belastbaren Schätzungen zur Dauer der Wiederherstellzeiten abgeben. Folglich benötigen die Nutzer von IT eigene Notfallpläne für die Aufrechterhaltung des Betriebs ihrer Einrichtungen und Fachabteilungen. Diese Pläne sind aber nicht Aufgabe der IT, sondern Aufgabe des Herrn der lokalen Organisation mit der entsprechenden Prozesskompetenz. Am Ende wird wohl schlichtweg Papier in Schubladen bereitliegen müssen. ■

MICHAEL THOSS

ist Gründungs- und Vorstandsmitglied des Bundesverbandes der Krankenhaus-IT-Leiterinnen / Leiter e.V. (www.kh-it.de) sowie Leiter der Informationstechnik der DRK Kliniken Berlin.

ANZEIGE

Patientendaten auf dem SCHWARZMARKT

Der Gesundheitssektor und damit sensible Patientendaten sind längst im Fokus von Datendieben. Noch ist Deutschland nicht so betroffen wie die USA, doch es ist höchste Zeit, aus den bisherigen Erfahrungen zu lernen.

TEXT: CHRISTINA CZESCHIK

Das Jahr 2015 war ein schwarzes Jahr für den US-amerikanischen Gesundheitssektor. Der Versicherer Anthem, Inc. wurde Opfer des größten Raubs von Gesundheitsdaten aller Zeiten: 80 Millionen Datensätze von Versicherten und Angestellten wurden von unbekannten Angreifern erbeutet. Andere Zwischenfälle betrafen die Non-Profit-Versicherer Premera Blue Cross und Excellus Blue Cross Blue Shield (11 bzw. 10 Millionen Datensätze) sowie das UCLA Medical Center (4,5 Millionen Datensätze). Da die Diebe zum Teil beträchtlichen Aufwand trieben, um an die Daten zu gelangen, stellt sich die Frage: Cui bono?

Mit gestohlenen Kreditkartendaten wird auf dem Schwarzmarkt reger Handel betrieben – so weit, so bekannt. Die Preise für einen Datensatz variieren dabei zwischen ein- und dreistelligen US-Dollar-Beträgen [1]. Auch mit anderen persönlichen Daten handeln Datenhehler: Beliebt sind neben Kreditkartendaten auch Login-Informationen für Shoppingseiten, E-Mail-Zugangsdaten sowie Geburtsdaten und Telefonnummern, die zum Zweck des Identitätsdiebstahls eingesetzt werden können.

Dieser Datenschwarzmarkt findet hauptsächlich im sogenannten Darknet statt, auf Webseiten, die von den herkömmlichen Suchmaschinen nicht indexiert werden und nur über anonymisiertes Surfen, beispielsweise mithilfe des Tor-Netzwerks [2], zugänglich sind. Neben gestohlenen Daten werden dort auch physische Waren wie Drogen, verschreibungspflichtige Medikamente und Waffen gehandelt. Über die Szene hinaus bekannt wurde der Fall des Marktplatzes Silk Road, dessen Initiator Ross Ulbricht 2013 verhaftet wurde.

Zunehmend finden nun auch Gesundheitsdaten ihren Weg auf die Schwarzmärkte des Darknet. Im Juni 2016 wurde das bislang größte Volumen an gestohlenen Patientendaten auf dem Marktplatz TheRealDeal angeboten (s. Abbildung 1). Der anonyme Verkäufer, der sich selbst thedarkoverlord nannte, bot am 26.06.2016 drei Datenbanken mit medizinischen Daten zum Verkauf an, eine 48 000 Patienten umfassende Datenbank einer Klinik in Farmington, Missouri, für 151 Bitcoin (ca. 100 000 US-Dollar), eine 210 000 Patienten umfassende Datenbank einer Klinik an einem unbezeichneten Ort im Mittleren Westen der USA für 303 Bitcoin (ca. 200 000 US-Dollar) und eine 397 000 Patienten umfassende Datenbank einer Klinik in Georgia für 607 Bitcoin (ca. 400 000 US-Dollar).

Die erstgenannte Klinik wurde später als Midwest Orthopedic Group identifiziert, die letztgenannte als Athens Orthopedic Clinic (AOC). Die elektronischen Patientenakten enthielten unter anderem Anamnesen einschließlich zurückliegender Operationen, Familienanamnesen, Allergien, aktuelle Diagnosen und aktuelle Medikation (s. Abbildung 2), zusätzlich zu administrativen Daten wie Namen, Adressen, Telefonnummern, ethnische Zugehörigkeiten, Versicherungsstatus und zuständige Apotheken.

Kurze Zeit später legte der Verkäufer nach. Am 28.06.2016 bot er eine 9,3 Millionen Datensätze umfassende Datenbank zum Preis von 750 Bitcoin (ca. 485 000 US-Dollar) an. Quelle der Datenbank sei ein großer

Krankenversicherer in den Vereinigten Staaten. Diese Datenbank enthielt keine medizinischen Aufzeichnungen, lediglich Namen, physische Adressen und E-Mail-Adressen, Telefonnummern, Geburtsdaten und Sozialversicherungsnummern. Berichtet wurde über das Angebot erstmals vom Online-Portal Deepdotweb, das News über die Märkte des Darknet sammelt.

Über einen anonymen Chat nahmen die Reporter von Deepdotweb persönlichen Kontakt zu thedarkoverlord auf. Dieser gab auf Nachfrage hin die Schwachstellen an, die er ausgenutzt habe, um an die Daten zu gelangen. Er habe, so berichtete er, die betroffenen Organisationen zunächst kontaktiert, um Lösegelder zwischen 100 000 und einer Million US-Dollar zu verlangen. Nachdem alle Opfer die Zahlung abgelehnt hatten, habe er sich dazu entschieden, die Daten zum Verkauf anzubieten.

Ob die angebotenen Datenbanken einen Käufer gefunden haben, ist nicht bekannt. Der Anbieter hatte dem Käufer exklusive Nutzung der erworbenen Daten und einen Verzicht auf anderweitige Veröffentlichung versprochen. Dass die Daten der AOC in Teilen öffentlich gemacht wurden und noch Mitte August im Web frei zugänglich waren [3], deutet darauf hin, dass zumindest diese Datenbank nicht verkauft wurde. Es bleibt jedoch die Frage, wer von einem Kauf von medizinischen Daten profitieren würde. Anders formuliert: Was ist das Geschäftsmodell hinter der Hehlerei mit medizinischen Daten?

Diverse Geschäftsmodelle

Der Mitgründer des oben genannten Tor-Netzwerks, Paul Syverson, sagte im Mai 2016 in einem Interview mit

»Zunehmend finden nun auch Gesundheitsdaten ihren Weg auf die Schwarzmärkte des Darknet.«

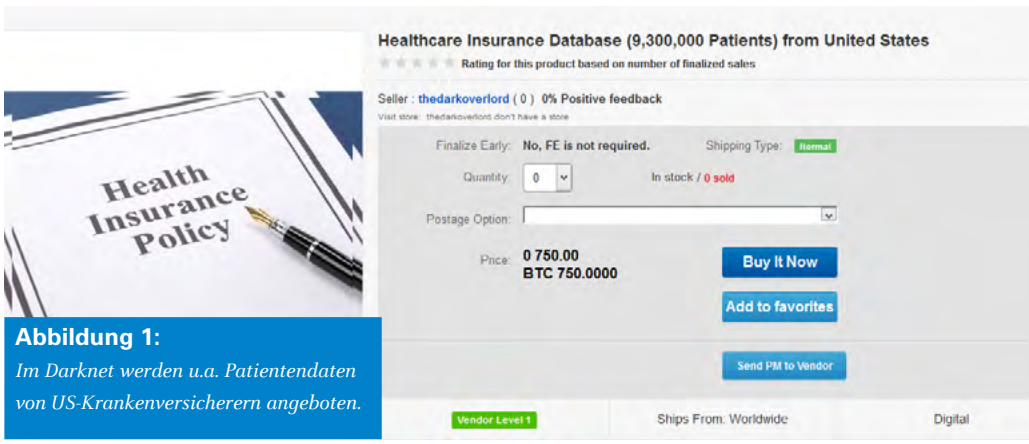


Abbildung 1:
Im Darknet werden u.a. Patientendaten von US-Krankenversicherern angeboten.

The Huffington Post [4], dass gestohlene Gesundheitsdaten in erster Linie für Identitätsdiebstahl im Gesundheitswesen verwendet werden. Dies ist ein Modell, das vor allem in den Vereinigten Staaten relevant ist: Ein relativ großer Anteil der Bevölkerung ist nicht krankenversichert oder unterversichert und kann also theoretisch von der Nutzung der persönlichen Daten einer versicherten Person profitieren. Im deutschen Gesundheitssystem scheint der Anreiz zu einem derartigen Datenmissbrauch im Moment gering.

Eine weitere Form des Identitätsdiebstahls ist jedoch auch für Deutschland relevant, der Identitätsdiebstahl mit dem Ziel, Kontrolle über fremde Bankkonten, Kreditkarten oder Konten für das Online-Shopping zu erhalten. Nicht-medizinische Informationen in elektronischen Patientenakten wie Adressen, Geburtsdaten und Bankverbindungen können auch bei uns zum Zwecke des Identitätsdiebstahls eingesetzt werden.

Eine weitere Einsatzmöglichkeit von unrechtmäßig erworbenen Daten illustriert schon das obige Beispiel von thedarkoverlord, nämlich Erpressung der betroffenen Institutionen oder Einzelpersonen. Von Ransomware-Attacken unterscheidet sich diese Art der Erpressung dadurch, dass die Daten für die Opfer weiterhin zugänglich bleiben. Die Drohung besteht vielmehr darin, die Daten öffentlich zu machen, mit dem damit einhergehenden Gesichtsverlust und – im Falle von Institutionen – möglichen juristischen Konsequenzen. Zumindest in den Vereinigten Staaten scheinen Krankenhäuser das Risiko von Klagen jedoch in Kauf zu nehmen, da solche kaum jemals mit einem Schuldspruch enden [5].

Ein Spezialfall, in dem konkret mit der Veröffentlichung privater Daten Gewinn gemacht wird, ist der Verkauf von medizinischen Informationen prominenter Patienten an die Boulevardpresse. Hierbei handelt es sich aber wohl eher um >

Bild: © https://www.deepdotweb.com/2016/06/28/now-9300000-healthcare-insurance-database-sold/

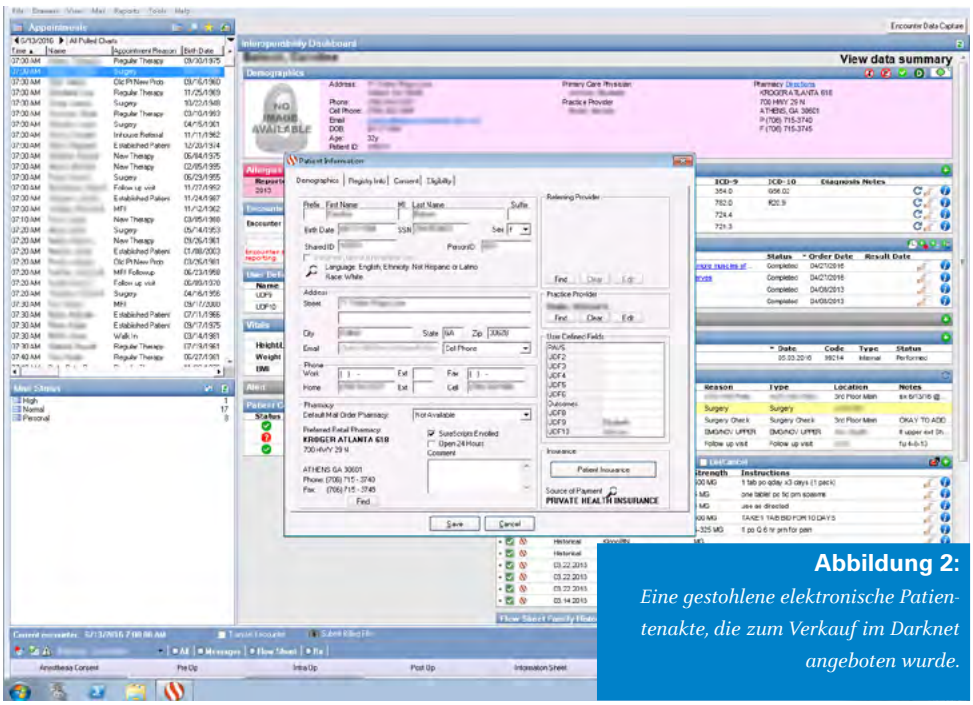


Abbildung 2:
Eine gestohlene elektronische Patientenakte, die zum Verkauf im Darknet angeboten wurde.

»Deutsche Kliniken und Versicherer scheinen im Vergleich zu ihren US-amerikanischen Cousins bisher wenig im Fokus von Angreifern zu stehen.«

gezielte Beutezüge, die oft von Mitarbeitern mit regulärem Zugang zu den Daten statt durch Cyberangriffe realisiert werden.

Ein weiteres Geschäftsmodell ist der Verkauf von persönlichen Daten an private Unternehmen, die diese zum Zwecke des Marketings verwenden. Wie die britische Zeitung Daily Mail berichtete, verkaufte die Firma Data Bubble vertrauliche Gesundheitsinformationen an Direkt-Marketer. Die betroffenen Personen erhielten daraufhin bis zu 20 unerwünschte Werbeanrufe pro Tag [6]. Die Daten stammen jedoch, soweit bekannt, nicht aus Datenleaks von Krankenhäusern, sondern von Versicherungsunternehmen, Fluggesellschaften und aus dem Heilmittel-Versandhandel.

Schließlich gehen Analysten davon aus, dass es eine weitere Gruppe von Interessenten und potenziellen Käufern von Gesundheitsdaten gibt, nämlich ausländische Geheimdienste. Konkret vermuten US-Geheimdienste im Fall des oben genannten Anthem-Hacks, dass die chinesische Regierung die Angreifer beauftragt haben könnte [7]. Der Diebstahl von Gesundheitsinformationen könne dabei einem doppelten Zweck dienen, einerseits der Industriespionage und dem Ausforschen der Verteidigungsmechanismen der betroffenen Organisationen, andererseits dem Sammeln kompromittierender Informationen, um in Zukunft vertrauliche Informationen von den betroffenen Individuen zu erpressen.

Sind diese Erkenntnisse auf Deutschland übertragbar? Auch deutsche Krankenhäuser waren in der Vergangenheit von Datenleaks betroffen. Ob jemals Daten deutscher Patienten auf den internationalen Schwarzmärkten aufgetaucht sind, ist nicht gesichert. Naturgemäß ist von einer hohen Dunkelziffer auszugehen. Deutsche Kliniken und Versicherer scheinen aber im Vergleich zu ihren US-amerikanischen Cousins bisher wenig im Fokus von Angreifern zu stehen. Das mag auch an der weniger fortgeschrittenen Digitalisierung im Gesundheitswesen liegen. Fazit: Jetzt ist ein guter Zeitpunkt, um rechtzeitig aus den Versäumnissen der anderen zu lernen. ■

DR. MED. CHRISTINA CZESCHIK
ist Ärztin für Medizinische Informatik.

LITERATUR-VERZEICHNIS

[1] http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/#section-3

[2] https://www.torproject.org

[3] https://www.databreaches.net/athens-orthopedic-clinic-patient-data-still-exposed-on-leak-site/

[4] http://www.huffingtonpost.com/entry/paul-syverson-tor-interview_

Bild: © EHR1.PNG: HTTPS://WWW.DEEPDOTWEB.COM/2016/06/26/655000-HEALTHCARE-RECORDS-PATIENTS-BEING-SOLD/

Im Fokus der Hacker: GESUNDHEITSDATEN

Immer mehr Menschen nutzen Gesundheitsapps für die eigene Gesundheits- und Fitnessüberwachung. Damit sammeln sie wertvolle Daten, die zunehmend für Cyberkriminelle interessant werden. Auch Kliniken geraten stärker ins Visier von Hackern. Da sind Maßnahmen zum Datenschutz dringend gefragt.

TEXT: KARSTEN KRUPNA

Laut Ergebnissen einer im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz durchgeführten Online-Befragung von ca. 2000 Verbrauchern nutzen derzeit 17 Prozent der Befragten eine sogenannte Gesundheits-App. Die oft z.B. als persönlicher „Fitnesscoach" genutzten Apps enthalten umfangreiche Gesundheitsdaten über die jeweiligen Nutzer. Diese bereits nach dem Bundesdatenschutzgesetz als besonders schützenswert eingestuften „besonderen Arten personenbezogener Daten" sind nicht nur für Ärzte und Krankenkassen interessant. Auch Hacker haben diese Daten im Fokus.

Healthcare-Branche auf Spitzenplatz für gefährdete Industrien

Obwohl über Gesundheits-Apps besonders sensible Daten der Nutzer verarbeitet werden, sind die datenschutzrechtlichen Anforderungen zum Schutz dieser Daten oft nicht eingehalten. Die Konferenz der unab- >

© LOGO3IN1 – FOTOLIA

hängigen Datenschutzbehörden des Bundes und der Länder hatte daher bereits im April 2016 datenschutzrechtliche Anforderungen zum Schutz von Gesundheitsdaten veröffentlicht. Sie fordern beispielsweise den Einsatz datenschutzfreundlicher Technologien und Voreinstellungen, um eine anonyme bzw. pseudonyme Datenverarbeitung zu ermöglichen. Die Betroffenen (Nutzer) sollen die Möglichkeit haben, die Übermittlung von Gesundheitsdaten an Dritte technisch zu unterbinden, sofern die Übermittlung nicht (z.B. wegen einer medizinischen Behandlung) erforderlich ist. Darüber hinaus stellt die Datenschutzkonferenz noch einmal ausdrücklich klar, dass gesetzliche Vorschriften zur Datensicherheit und Vertraulichkeit von Daten nicht durch Verträge oder Einwilligungserklärungen abbedungen werden können.

Die besondere Notwendigkeit, Gesundheitsdaten zu schützen, zeigt sich insbesondere in dem Bedrohungsrisiko durch Cyberkriminelle. Ausweislich des Cyber Security Intelligence Index 2016 von IBM steht die Healthcare-Branche auf Platz eins der am meisten attackierten Industrien.

Technischer Datenschutz schafft Vertrauen und schützt vor Cyberangriffen

Je häufiger erfolgreiche Cyberangriffe auf Gesundheits-Apps bekannt werden, desto mehr stellen Nutzer die praktischen Vorteile dieser Apps infrage. IT-Sicherheit spielt damit bei der Vertrauensbildung aufseiten der Kunden und der Entwicklung des Vertriebs dieser Apps eine zentrale Rolle. App-Entwickler und App-Anbieter sollten sich daher mit dem technischen Datenschutz sorgfältig auseinandersetzen. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat hierzu einen Prüfkatalog veröffentlicht, der eine individuelle Prüfung zwar nicht ersetzt, jedoch zumindest eine erste Orientierungshilfe bietet.

Haftungsrisiken für die Klinik-Geschäftsleitung

Cyberkriminelle haben es nicht „nur“ auf die Daten aus den Apps abgesehen. Vielmehr geraten zunehmend auch die Krankenhäuser selbst in das Visier der Täter. Ziel ist es dabei, z.B. durch den Einsatz von Schadsoftware („Ransomware“) zunächst die Daten der Patienten bzw. Krankenhäuser zu verschlüsseln und anschließend ein Lösegeld für die Entschlüsselung zu fordern. Berücksichtigt man in diesem Zusammenhang die geringe Aufklärungsquote bei Hackerangriffen, ist zukünftig noch von einer wachsenden Bedrohung auszugehen. Die Geschäftsleitung sollte daher unbedingt – sofern noch nicht geschehen – die unternehmensspezifische Gefährdungslage analysieren und entsprechende Schutzmaßnahmen ergreifen.

Nach dem IT-Sicherheitsgesetz sind Betreiber von „kritischen Infrastrukturen“ sogar verpflichtet, Mindeststandards für die IT-Sicherheit zu beachten, um ihre Systeme insbesondere vor Cyberangriffen zu schützen. Zudem müssen erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden. Nachdem durch die am 3. Mai 2016 in Kraft getretene Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) zunächst eine Bestimmung der „Kritischen Infrastrukturen“ in den Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung erfolgte, soll dies bis Anfang 2017 per Änderungsverordnung auch für die Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen erfolgen. Dabei ist zu erwarten, dass insbesondere Krankenhäuser ausdrücklich dem Gesundheitssektor zugeordnet werden. Verletzt die Geschäftsleitung ihre Pflichten zum Schutz der IT-Infrastruktur, kommen Schadenersatzansprüche der durch den Hacker-angriff geschädigten Gesellschaft in Betracht (vgl. z.B. § 93 Abs. 2 Satz 1 AktG bzw. § 43 Abs. 2 GmbHG). An dieser Stelle sei erwähnt, dass sich an dieser Zuordnung auch nach der Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union „NIS-Richtlinie“ nichts ändern wird. Vielmehr sind Krankenhäuser in dem vorgenannten Entwurf bereits explizit benannt.

Praxishinweise

IT-Sicherheitsmaßnahmen stellen einen zentralen Faktor zum Schutz vor Cyberangriffen dar. Einen hundertprozentigen Schutz kann es allerdings nicht geben. Ziel kann nur die Maximierung des Schutzes sein. Daher sollten neben den IT-Sicherheitsmaßnahmen zusätzlich organisatorische Maßnahmen getroffen werden, um einen effizienten und gesetzeskonformen Umgang mit einem Hackerangriff zu gewährleisten.

Auch ohne Betreiber einer Kritischen Infrastruktur i.S.d. IT-Sicherheitsgesetzes zu sein, haben bereits nach dem geltenden Bundesdatenschutzgesetz (BDSG) Unternehmen im Falle von Datenschutzverletzungen, wie z. B. Hackerangriffen,

umfangreiche Informationspflichten nach dem Bundesdatenschutzgesetz zu beachten (§ 42a BDSG). Eine Verletzung dieser Meldepflichten kann mit einem Bußgeld bis zu 300 000 Euro geahndet werden. Dabei sei nach aktueller Auffassung des BayLDA der für die Bestimmung des Bußgeldrahmens maßgebliche „weltweite Jahresumsatz" unter Berücksichtigung der gesamten Unternehmensgruppe bzw. des gesamten Konzerns und nicht lediglich anhand des jeweils Verantwortlichen bzw. Auftragsverarbeiters zu bestimmen.

Die neue EU-Datenschutzgrundverordnung (DSGVO), die am 25. Mai 2018 in Kraft tritt, sieht gemäß Art. 33, 34 DSGVO bei Datenschutzverletzungen ebenfalls umfassende Meldepflichten gegenüber der Aufsichtsbehörde und den betroffenen Personen vor. Bei einer Pflichtverletzung droht den Unternehmen dann sogar ein Bußgeld in Höhe von bis zu zehn Millionen Euro oder zwei Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher der Beträge höher ist (Art. 83 Abs. 4 DSGVO).

Unternehmen, die den Vorfall lieber verschweigen und damit zumindest einen Reputationsschaden abwenden wollen, ist diese „Vogel-Strauß-Strategie" keinesfalls zu empfehlen. Ungeachtet des drohenden Bußgeldes bei einer Verletzung der Meldepflichten ist nicht ausgeschlossen, dass die Täter im Rahmen einer Erpressung gezielt mit der Veröffentlichung von Daten drohen und zur Verstärkung der Drucksituation einzelne Daten im Internet veröffentlichen. Darüber hinaus müssen die unternehmensinternen Schwachstellen berücksichtigt werden. Bereits ein frustrierter Mitarbeiter genügt und der Vorfall wird z.B. über die sozialen Netzwerke oder durch eine Meldung an die Presse bekannt. Die Wahrscheinlichkeit, dass der Hackerangriff also öffentlich wird, ist relativ hoch. Zeigt sich dann, dass das Unternehmen den Datenvorfall bewusst verschweigen wollte, dürfte der Reputationsschaden – den es ursprünglich zu vermeiden galt – wesentlich höher sein.

»Je häufiger erfolgreiche Cyberangriffe auf Gesundheits-Apps bekannt werden, desto mehr stellen Nutzer die Vorteile der Apps infrage.«

Um die notwendige Pflichterfüllung sicherzustellen, sollte zum Beispiel ein „Präventionsteam Cybercrime" etabliert werden, das das bestehende Konzept gegen Cyberangriffe zunächst bewertet, sofern erforderlich anpasst und sodann regelmäßig erneut überprüft. Schließlich kann auch die Prüfung der bestehenden Versicherungsverträge auf deren Deckungsumfang durchaus empfehlenswert sein und gegebenenfalls der Abschluss einer sogenannten Cyberversicherung in Betracht gezogen werden.

Präventiv muss regelmäßig Folgendes betrachtet werden:

- Prüfung der Datenverarbeitungsprozesse sowie der technischen und organisatorischen Maßnahmen auf Gesetzeskonformität,
- Identifizierung und Minimierung besonders riskanter Sachverhalte unter Berücksichtigung der Sensibilität der Daten,
- Anpassung und Schulung der IT-Richtlinien für alle Mitarbeiter,
- Prüfung der Notwendigkeit und des Umfanges eines Versicherungsschutzes,
- Etablierung eines Krisenstabes und Maßnahmenkatalogs für den Fall eines Cyberangriffs,
- kontinuierliche Auswertung aller informell oder öffentlich bekannt gewordenen Schadensfälle im Sinne einer „lernenden Organisation".

Im Falle eines Cyberangriffs hat der Krisenstab neben IT-technischen Maßnahmen zur Prävention weiterer Angriffe ein umfangreiches Szenario abzuarbeiten:

- Beachtung gesetzlicher und vertraglicher Informationspflichten (z.B. gegenüber Betroffenen, der Aufsichtsbehörde für den Datenschutz oder dem BSI),
- Prüfung und Abwehr von Schadenersatzansprüchen betroffener Personen,
- Prüfung und Durchsetzung von Schadenersatzansprüchen gegen einen Vertragspartner wegen einer Vertragsverletzung,
- Stellung einer Strafanzeige,
- Prüfung und Durchsetzung von Schadenersatzansprüchen gegen den Täter,
- Geltendmachung des Versicherungsschadens,
- Abstimmung der Öffentlichkeitsarbeit. ■

DR. KARSTEN KRUPNA

ist Rechtsanwalt bei Esche Schümann Commichau in Hamburg und berät nationale und internationale Unternehmen insbesondere in den Bereichen Datenschutz, IT-Recht und Cybersecurity.

Fordern Sie Ihr kostenloses Probeheft an und überzeugen Sie sich selbst

E-HEALTH-COM

Das unabhängige Fachmagazin für HEALTH-IT, Telemedizin und vernetzte Medizintechnik

Beate Gehm, Anzeigenleitung,
Tel.: + 49 (0)69 840006 - 3030
b.gehm@health-care-com.de

oder direkt online:
www.e-health-com.eu/abo/

5 Schritte für SICHERE IT-SYSTEME

Mit der Einführung der elektronischen Patientenakte und den aktuellen Cyberangriffen auf Gesundheitseinrichtungen rückt die Datensicherheit immer weiter in den Vordergrund. Mit diesen 5 Tipps lässt sich die Umstellung der IT meistern und die Sicherheit erhöhen.

1. Schulungen der IT-Beauftragten und der Mitarbeiter

Stellen Sie sicher, dass ihre IT-Beauftragten sich um die Anlagen und Systeme sorgsam kümmern und diese verantwortungsvoll pflegen. Regelmäßiges White-Hacking kann die Sicherheit erhöhen, denn so können Lücken entdeckt werden, noch bevor mögliche Angreifer sie finden. Auch Schulungen der Mitarbeiter sind wichtig. Mitarbeiter gelten immer noch als unsicherste Stelle der IT. Der Umgang mit BYOD und die Internetnutzung müssen klar geregelt sein.

2. Gefahren ermitteln und Lösungen finden

Welchen Gefahren ist mein System ausgesetzt und welche Maßnahmen können ergriffen werden? Das sollte immer wieder neu ermittelt werden, damit entsprechende Maßnahmen ergriffen werden können. Vor allem in Gesundheitseinrichtungen müssen sich Mitarbeiter meist eine Vielzahl sehr komplizierter Passwörter merken. Der Schritt, diese auf einem Zettel oder in seinem Smartphone zu notieren, ist schnell getan und eine neue Sicherheitslücke geschaffen. Mit Single-Sign-On-Lösungen können solche Lücken geschlossen werden.

3. Die richtigen Systeme finden

Um die Arbeitsabläufe in Gesundheitseinrichtungen nicht zu stören, sondern zu vereinfachen, gilt es die richtigen Systeme zu finden. Die Lösungen müssen in das bestehende IT-System passen, hohe Datensicherheit bieten und die Bedürfnisse von Mitarbeitern und Patienten erfüllen. Bei der Umsetzung von IT-Systemen sind vor allem die ersten Schritte entscheidend. Die Integration in bestehende Systeme und der Durchlauf der Testphasen, bevor eine Lösung im Alltag eingesetzt wird, sollte immer mit einem im Krankenhaus erfahrenen Partner erfolgen. Eine solide Bereitstellung, Schulung und Optimierung sind im Lebenszyklus eines Technologie-Produkts ausschlaggebend, um die mit neuen Technologien einhergehenden Risiken zu minimieren.

4. Zugriffsrechte und verschlüsselte Datenübertragung

Authentifizierungs-Management-Lösungen erleichtern durch eine Chipkarte oder durch moderne 3D-Gesichtserkennungslösungen den Zugriff auf Daten, ohne dass sich Mitarbeiter weitere Zugangsdaten merken müssen. So gibt es heute bereits Systeme, die den schnellen Zugriff auf virtuelle Desktops an verschiedenen Arbeitsplätzen ermöglichen und den klinischen Mitarbeitern folgen, während diese sich innerhalb des Krankenhauses bewegen.

5. Aktualität für mehr Sicherheit

Wenn Systeme länger nicht auf dem neuesten Stand sind, führt das zu mehr Problemen. Nicht nur Hacker haben leichteres Spiel, auch die Systeme funktionieren nicht mehr reibungslos, was zu einem erschwerten Arbeitsablauf führen kann. ■

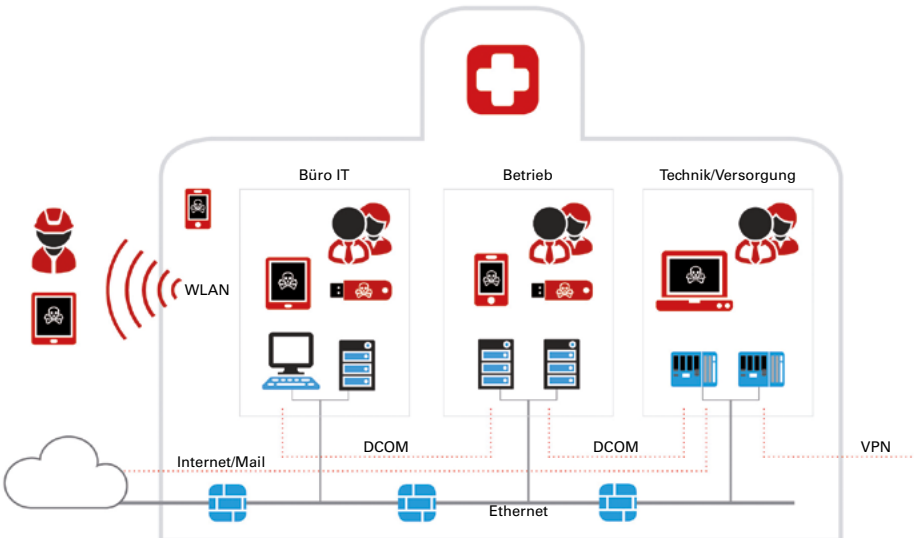
IMPRIVATA

Dr. Frank Lampe, Marketing Director EMEA & APAC

Zeltner Str. 1- 3, 90443 Nürnberg

Tel.: +49- 911 8819 7330
flampe@imprivata.com
www.imprivata.com

Effizienter Schutz nach dem IT-SICHERHEITSGESETZ



Gefahrenpotenzial im Krankenhaus-Netzwerk

Das vom Bundestag beschlossene „Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme“ (IT-Sicherheitsgesetz) ist mit Wirkung zum 25. Juli 2015 in Kraft getreten. Es betrifft eine erhebliche Anzahl von großen Betreibern „Kritischer Infrastrukturen“ (KRITIS). Darunter zählen auch Krankenhäuser. Hilfestellung leistet hier das Unternehmen Videc, welches sein Know-how für vernetzte und sensible Prozessleittechnik in der Industrie auch für Krankenhäuser zur Verfügung stellt.

Entsprechend dem neuen IT-Sicherheitsgesetz „ITSiG“ müssen die Betreiber kritischer Infrastrukturen künftig nicht nur einen Mindeststandard an IT-Sicherheit einhalten und nachweisen, sondern auch erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Der sorglose Einsatz von internetfähigen IT-Systemen wie Smartphones und Tablets führt zu einem ungeahnten Ausmaß an Sicherheitslücken. Dazu gehören auch alle Komponenten mit USB-Anschluss, da zum Beispiel USB-Speicher-Sticks an internetfähigen PC stecken können. Ein gutes Gerüst für den Aufbau eines Sicherheitsmanagements bieten insbesondere die Normen der ISO-27000-Reihe.

Das Risikomanagement gemäß IEC 80001 erfordert vom Betreiber medizinischer IT-Netzwerke eine Identifizierung der Bedrohungen und Schwachstellen. Diese Norm hat zunächst nur Empfehlungscharakter, sollte jedoch umgesetzt werden, um möglichen Haftungsansprüchen entgegenzuwirken. Es muss eine Möglichkeit der Risikopriorisierung implementiert sein, genauso wie ein Maßnahmenkatalog zur Behandlung der Risiken. Eine Unterstützung der regelmäßigen jährlichen Auditierung runden die Anforderungen ab.

Ein Produkt für den Bereich IT-Sicherheit auch in Krankenhäusern ist IRMA, welches sich bereits erfolgreich in Versorgungsbetrieben und in der Industrie bewährt. IRMA („Industrie Risiko Management Automatisierung“) ermöglicht es, die Verpflichtungen und Anforderungen nach dem „ITSiG“ umzusetzen – angepasst an die Unternehmensgröße und den finanziellen Rahmen. Dies erfolgt durch passives Scannen des Netzwerkes sowie die Analyse der IT-Assets und Verbindungen. Jede Verbindung und jedes Gerät kann validiert werden. Das Programm liefert Informationen für die Netzsegmentierung und die Trennung mit Firewalls. Zudem überwacht es kontinuierlich die Anlagen und bietet intelligente Alarmierungen.

IRMA ermöglicht bereits frühzeitig eine tief gehende Analyse ohne aufwendige Bestandsaufnahmen. Kurzfristig notwendige Optimierungsschritte lassen sich kosteneffizient initiieren. IRMA unterstützt die effiziente Erarbeitung und Umsetzung bei der Durchführung des Risikomanagements (ISO 9001-2015). Die Dokumentation des IT-Sicherheitskonzepts sowie die nach ISO 27000 notwendigen Berichte lassen sich umgehend in Angriff nehmen. Mit IRMA erhält der Betreiber schnell und ohne aufwendige Planung die für die Erfassung der Cyber-Assets sowie für das Erkennen und Melden von Angriffen notwendige Übersicht und Informationen. Durch die kontinuierliche Überwachung und einfache Validierung sowie Behandlung von IT-Schwachstellen werden die Anlagen im Krankenhaus umgehend besser geschützt. ■

VIDEC.
Videc GmbH
Contrescarpe 1
28203 Bremen
info@videc.de
www.videc.info

Health IT-Portal

IT-Lösungen im Gesundheitswesen. In einem Portal vereint.

Das Health-IT-Portal ist als umfangreicher Recherche- und Nachrichtenpool DIE PLATTFORM für alle Akteure der Branche

DIE BRANCHE
AUF EINEN KLICK

Nutzen Sie das Health-IT-Portal

ALS UNTERNEHMEN

Für Produkte und Dienstleistungen
Werden Sie Partner und bleiben Sie für die Interessenten der Branche präsent und aktuell

ALS ANWENDER

Für Information und Orientierung durch Vielfalt

www.health-it-portal.de

RS MEDICAL CONSULT

1. Expertenforum – IT-Sicherheit für Krankenhäuser/Kliniken

Risiken und Chancen der vernetzten IT

IT-Sicherheit braucht Strategie, Technik und Organisation

Save the Date!

23. November 2016 in Nürnberg

Le Méridien Grand Hotel Nürnberg
Bahnhofstraße 1-3 · 90402 Nürnberg

4 Fortbildungspunkte Kategorie C – Bayerische Landesärztekammer

RS Medical Consult GmbH Unternehmensberatung
Johann-Hammer-Str. 22 · 97980 Bad Mergentheim · Deutschland
Telefon +49 (0)7931 52612 · Fax +49 (0)7931 561226
info@rsmedicalconsult.com · www.rsmedicalconsult.com